

HSIN-CI New Posting: (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015

From: NICC HSIN-CI New Posting <CIISE.dhs@public.govdelivery.com>
To: mary.moore@cookcountyil.gov, Mary Moore (Sheriff)
</O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Mary.moore>
Sent: May 8, 2015 12:25:42 PM CDT
Received: May 8, 2015 12:27:56 PM CDT

All,

A new item, (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015, has been posted to the HSIN-Critical Infrastructure (CI) portal at <https://hsin.dhs.gov/ci/home/Pages/default.aspx> under Today's New Documents and/or Recent CI Documents section of the portal.

This product is intended to provide perspective to assist federal, state, local, and tribal government agencies and authorities, the private sector Critical Infrastructure Owners and Operators, and other entities to develop priorities for protective and support measures relating to an existing or emerging threat to homeland security.

Access to the site will require the use of your assigned HSIN-CI user name and password. Upon linking directly to the site, the user can then also navigate within HSIN-CI as well as within those Communities of Interest to which they have access.

If you need to update your HSIN password, please click <https://auth.dhs.gov/admin/faces/pages/forgotpwd.jsp> to be directed to a self-service portal. For technical assistance, you may contact the HSIN Help Desk at hsin.helpdesk@hq.dhs.gov or toll free at (866) 430-0162.

Opting-Out Procedure: If you would like to be removed from future HSIN-CI notifications, please click the link below.

Very respectfully,

NICC Watch Operations
Department of Homeland Security
202-282-9201
NICC@dhs.gov

You are subscribed to NICC HSIN-CI New Posting for CI Information Sharing Environment. This information has recently been updated, and is now available.

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

[Unsubscribe](#)



HSIN-CI New Posting: (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015

From: NICC HSIN-CI New Posting <CIISE.dhs@public.govdelivery.com>
To: michael.fonseca@cookcountyl.gov, Michael Fonseca (Sheriff)
</O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Michael.fonseca>
Sent: May 8, 2015 12:25:42 PM CDT
Received: May 8, 2015 12:44:31 PM CDT

All,

A new item, (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015, has been posted to the HSIN-Critical Infrastructure (CI) portal at <https://hsin.dhs.gov/ci/home/Pages/default.aspx> under Today's New Documents and/or Recent CI Documents section of the portal.

This product is intended to provide perspective to assist federal, state, local, and tribal government agencies and authorities, the private sector Critical Infrastructure Owners and Operators, and other entities to develop priorities for protective and support measures relating to an existing or emerging threat to homeland security.

Access to the site will require the use of your assigned HSIN-CI user name and password. Upon linking directly to the site, the user can then also navigate within HSIN-CI as well as within those Communities of Interest to which they have access.

If you need to update your HSIN password, please click <https://auth.dhs.gov/admin/faces/pages/forgotpwd.jsp> to be directed to a self-service portal. For technical assistance, you may contact the HSIN Help Desk at hsin.helpdesk@hq.dhs.gov or toll free at (866) 430-0162.

Opting-Out Procedure: If you would like to be removed from future HSIN-CI notifications, please click the link below.

Very respectfully,

NICC Watch Operations
Department of Homeland Security
202-282-9201
NICC@dhs.gov

You are subscribed to NICC HSIN-CI New Posting for CI Information Sharing Environment. This information has recently been updated, and is now available.

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

[Unsubscribe](#)



**HSIN-CI New Posting: (U//FOUO) RCR: Criminal Hackers Target Police to Protest
Perceived Injustices, dated 08 May 2015**

To: Michael Fonseca (Sheriff)
Sent: May 8, 2015 12:25:42 PM CDT
Received: May 8, 2015 12:44:31 PM CDT

**HSIN-CI New Posting: (U//FOUO) RCR: Criminal Hackers Target Police to Protest
Perceived Injustices, dated 08 May 2015**

To: Mary Moore (Sheriff)
Sent: May 8, 2015 12:25:42 PM CDT
Received: May 8, 2015 12:27:56 PM CDT

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

From: Alana_Sorrentino@isp.state.il.us
To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:54 PM CDT
Received: May 8, 2015 12:57:42 PM CDT
Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived Injustices 05082015.pdf

Please see attached the Roll Call Release, "Criminal Hackers Target Police to Protest Perceived Injustices" dated May 8, 2015.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and cannot verify the contents to be factual. If you have any questions reference, this information, please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

Alana Sorrentino
Emergency Management Intelligence Officer | Statewide Terrorism & Intelligence Center
Liaison| Illinois Emergency Services Management Association (IESMA)
Western Illinois University | Illinois Terrorism Task Force
2200 South Dirksen Parkway, Springfield, IL 62703, Suite 238
Office Phone: 217-558-3739 | IESMA Phone: 217-557-4772
Email: Alana.Sorrentino@illinois.gov | Alana_Sorrentino@isp.state.il.us

FW: (UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

From: Bill Martin <BMartin@schillerparkil.us>

To:

'Amy Kreml' <akreml@wooddale.com>, 'Ann Montgomery' <amontgomery@getipass.com>, 'Anthony Garvey (Chief)' <agarvey@northriverside-il.org>, 'Anthony Gennett' <agennett@ci.berwyn.il.us>, 'Anthony Greco' <agreco@melroseparkpd.com>, 'Anthony Milazzo' <tmilazzo@hillside-il.org>, 'Anthony Raitano' <araitano@parkridgepolice.org>, 'B Beck' <beckb@vil.bloomingtondale.il.us>, 'Ben Kadolph' <bkadolph@oak-brook.org>, 'Bill Foster' <bfoster@darien.il.us>, 'Bill Frese' <wfrese@wooddale.com>, 'Bill Martin' <BMartin@schillerparkil.us>, 'Bill Stack' <william.stack@usss.dhs.gov>, 'Bob Mance' <ofcmance@yahoo.com>, 'Brad Mann' <bmann@ci.berwyn.il.us>, 'Brent Hoekstra' <bhoekstra@berkeley.il.us>, 'Brian Cantwell' <bcantwell@ci.berwyn.il.us>, 'Brian Dooley' <dooleyb@bensenville.il.us>, 'Brian Greenenwald' <bgreenenwald@riverside.il.us>, 'Brian Strockis' <bstockis@oak-brook.org>, 'Bruce Mason' <masonb@vil.bloomingtondale.il.us>, 'Carlos Garcia' <cgarcia@northriverside-il.org>, 'Carmelita Terry' <cterry@ci.berwyn.il.us>, 'Carol Dundovich' <CDundovich@bensenville.il.us>, 'Charles Schauer' <cschauer@ci.berwyn.il.us>, 'Chief Sam Pitassi' <Spitassi@melroseparkpd.com>, 'Chris Banaszynski' <cbanaszynski@wooddale.com>, 'Chris Mowinski' <cmowinski@northlakecity.com>, 'Chris Pavini' <detectives@stoneparkpd.com>, 'Christopher Boenzi' <cboenzi@northriverside-il.org>, 'Chuck Leuver' <cleuver@villageofhinsdale.org>, 'Cmndr Robert Nicholas' <Robert.Nicholas@Elmhurst.org>, 'Corey O'Neal' <coneal@vil.bellwood.il.us>, 'Countryside Police Department' <police@countrysidepolice.org>, 'Curt Novak' <cnovak@indianheadpark-il.gov>, 'D. Ransom' <dransom@elmwoodpark.org>, 'Damian Villagomez' <rgdetect1@vrg.us>, 'Dan Albrecht' <dalbrecht@wsprings.com>, 'Dan Bresnahan' <dbresnahan@berkeley.il.us>, 'Dan Groth' <daniel.grothjr@cookcountyil.gov>, 'Daniel Haxton' <daniel.haxton@getipass.com>, 'Daniel Murphy' <dmurphy@hillside-il.org>, 'Daniel Pereda' <dpereda@hillside-il.org>, 'Daniel Romanski' <dromanski@northlakecity.com>, 'Dave Krull' <dkrull@riverside.il.us>, 'Dave Rivkin' <dave.rivkin@elmhurst.org>, 'Dave Rohlicek' <drohlicek@villageoflagrange.com>, 'David Clark' <dclark@oakbrookterrace.net>, 'David Green' <dgreen@ci.berwyn.il.us>, 'David Kudla' <dkudla@brookfieldil.gov>, 'David MacArtney' <dmacartney@oakbrookterrace.net>, 'David Martin' <dmartin@vil.bellwood.il.us>, 'Deborah Garcia' <dgarcia@northriverside-il.org>, 'Dion Bobo' <dbobo@northriverside-il.org>, 'Dominic Panico' <dominic.panico@elmhurst.org>, 'Don Batko' <sgtdb@hotmail.com>, 'Ed Coughlin' <ed.coughlin@elmhurst.org>, 'Ed Rompa' <erompa@lagrange.org>, 'Eric Katzin' <ekatzin@riverside.il.us>, 'Eric LoCoco' <elococo@westchesterpolice.com>, 'Erik Bernholdt' <ebernholdt@villageofhinsdale.org>, 'Fabian Navarro' <fnavarro@riverside.il.us>, 'Frank Cimaglia' <fcimaglia@ci.berwyn.il.us>, 'Frank DeSimone' <FDeSimone@schillerparkil.us>, 'Frank Fagiano (Chief)' <ffagiano@elmwoodpark.org>, 'Frank Giammarese' <giamf@vil.bloomingtondale.il.us>, 'Frank Homolka' <fhomolka@villageofhinsdale.org>, 'Frank Lara' <flara@riverside.il.us>, 'Frank Teutonico' <fteutonico@ci.berwyn.il.us>, 'Gary Pohanka' <gpohanka@amfam.com>, 'Gavin Zarbock' <gzarbock@ci.berwyn.il.us>, 'Genaro Manzo' <gmanzo@melroseparkpd.com>, 'George Zorzi' <gzorzi@lumc.edu>, 'Gerald Karceski' <gkarceski@burr-ridge.gov>, 'Gil Espinosa' <gespinosa@melrosepark.com>, 'Giordano Manfredini' <gmanfredini@ci.berwyn.il.us>, 'Greg Vesta' <gvesta@wooddale.com>, 'J. Drury (D.C.)' <JDrury@ci.berwyn.il.us>, 'J. Nowacki' <jnowacki@elkgrove.org>, 'J.Schillinger' <jschillinger@melroseparkpd.com>, 'Jack Bridson' <jbridson@vil.bellwood.il.us>, 'Jack Shannon' <jshannon@northlakecity.com>, 'Jake Pollard' <jpollard@northlakecity.com>, 'James Ferguson' <James.Ferguson@ic.fbi.gov>, 'James Lazansky' <jlazansky@riverside.il.us>, 'James Volpe' <jvolpe@wheaton.il.us>, 'James Wagner' <jwwagner@getipass.com>, 'Jason Moran' <jmoran@cookcountygov.com>, 'Jay Militello' <jmilitello@northlakecity.com>, 'Jeff Caldwell' <jc1489@rsmt.net>, 'Jeff Hill' <hillj@vil.bloomingtondale.il.us>, 'Jeff Juan' <jjuan@melroseparkpd.com>, 'Jeff Kucera' <jeff.kucera@elmhurst.org>, 'Jeff Sargent (Chief)' <jsargent@triton.edu>, 'Jesus Ramos' <jesus_ramos@cppoliceservice.com>, 'Jim Greenwood' <jgreenwood@river-forest.us>, 'Jim Nowicki' <jnowicki@melroseparkpd.com>, 'Jim Ritz (Chief)' <JRitz@ci.berwyn.il.us>, 'Jim Sassetti' <jsassetti@ci.berwyn.il.us>, 'Jim Schlicher' <jschlicher@westmont.il.gov>, 'Jim Sperandio' <jsperandio@oak-park.us>, 'Jimenez Allen' <jallen@vil.bellwood.il.us>, 'Jo Kujawinski' <jkujawinski@wheaton.il.us>, 'Jocelyn Ellis' <jocelyn.ellis@oci.fda.gov>, 'Joe Duca' <jduca@indianheadpark-il.gov>, 'Joe Maranowicz' <jmaranowicz@addison-il.org>, 'John Cairo' <jcairo@riverside.il.us>, 'John Dorner' <jdorner@parkridgepolice.org>, 'John Hadjioannou' <jhadjioannou@ci.berwyn.il.us>, 'John Helms' <jhelms@burr-ridge.gov>, 'John Kerner' <jkerner@berkeley.il.us>, 'John Krueger'

ridge.gov>, 'John Kerner' <jkerner@berkeley.il.us>, 'John Krueger' <kruegerj@vil.bloomington.il.us>, 'John Magnus' <jmagnus@ci.berwyn.il.us>, 'John Mudra' <jmudra@indianheadpark-il.gov>, 'John Trevarthen' <jtrevarthen@vil.bellwood.il.us>, 'Joseph Green' <jgreen@ci.berwyn.il.us>, 'Joseph Kanupke' <jkanupke@mountprospect.org>, 'Joseph Lukaszek' <jlukaszek@hillside-il.org>, 'Joseph Riordan' <riordan_j@cityofelgin.org>, 'Joseph Santangelo' <jsantangelo@ci.berwyn.il.us>, 'Juan Duarte' <jduarte@northlakecity.com>, 'Justin Patti' <jbtpatti@berkeley.il.us>, 'Karlas Robinzine' <krobinzine@ci.berwyn.il.us>, 'Kate O'Hara' <KATE.O'HARA@cookcountylil.gov>, 'Kathy Shaughnessy (LT)' <kshaughn@parkridgepolice.org>, 'Ken Beres' <kberes@northlakecity.com>, 'Ken Gross' <kgross@forestpark.net>, 'Ken Uher' <kuher@villageoflagrange.com>, 'Kenneth Howard' <khoward@ci.berwyn.il.us>, 'Kevin O'Connell' <koconnell@atg.state.il.us>, 'Kevin Susmarski' <ksusmarski@villageofhinsdale.org>, 'Kreg Floyd' <kfloyd@countysidepolice.org>, 'Kris Gardner' <kgardner@indianheadpark-il.gov>, 'L. Bartemio' <lbartemio@melroseparkpd.com>, 'LaGrange Park Detectives' <detective@lagrange.org>, 'Lane Niemann' <lniemann@northriverside-il.org>, 'Lee Zeitlin' <lee.zeitlin@czs.org>, 'Len Norek' <lnorek@berkeley.il.us>, 'Louis O'Rourke' <lorourke@oakbrookterrace.net>, 'M. Cimaglia (D.C.)' <MCimaglia@ci.berwyn.il.us>, 'M. Winiarczyk' <mjwiniarczyk@elmwoodpark.org>, 'Marc Loftus' <mloftus@burr-ridge.gov>, 'Mario Faso' <mfaso@parkridgepolice.org>, 'Mario Valkov' <mvalkov@northlakecity.com>, 'Mark Altobella' <maltobel@willowbrook.il.us>, 'Mark Astrella' <mastrella@elmwoodpark.org>, 'Mark Battaglia' <mbattaglia@countysidepolice.org>, 'Mark Bozek' <mbozek@darlen.il.us>, 'Mark Gallagher' <mgallagher@ci.berwyn.il.us>, 'Mark Van Stedum' <mvanstedum@addison-il.org>, 'Martin Milas' <mmilas@oakbrookterrace.net>, 'Mary Byrne' <byrne@oak-park.us>, 'Melody Rissman' <mrisman@wooddale.com>, 'Melrose Park P.D.' <info@melroseparkpd.com>, 'Michael Barnes' <mbarnes@burr-ridge.gov>, 'Michael Castellan (Dep. Chief)' <mcastellan@melroseparkpd.com>, 'Michael Fellows' <mfellows@ci.berwyn.il.us>, 'Michael Gaspari' <mgaspari@elkgrove.org>, 'Michael Hylton' <mhylton@oakbrookterrace.net>, 'Michael Keating' <mkeating@forestpark.net>, 'Michelle Glosky' <mglosky@burr-ridge.gov>, 'Michelle Strugala' <mstrugala@willowbrook.il.us>, 'Mike Coughlin' <mcoughlin@villageofhinsdale.org>, 'Mike Jones' <mjones@vofp.com>, 'Mike Peters' <mpeters@wooddale.com>, 'Mike Rivas' <mrivas@wooddale.com>, 'Mike Scudiero' <msscudiero@melroseparkpd.com>, 'Neil Reyes' <neil_reyes@cppoliceservice.com>, 'Nicholas Schiavone' <nschiavone@ci.berwyn.il.us>, 'Nick Petrovic' <npetrovic@forestpark.net>, 'O'hara Johnson' <ohara_johnson@yahoo.com>, 'P. Rocita' <pnocita@melroseparkpd.com>, 'Patricia McConnell' <pmcconnell@atg.state.il.us>, 'Paul Finer' <BlackHawkpaul1@comcast.net>, 'Paul Johnson' <paul.johnson@tigta.treas.gov>, 'Paul Retzke' <Paulretzke@comcast.net>, 'Pete Culafic' <pculafic@northriverside-il.org>, 'Pete Vizek' <pvizek@lyonspolice.org>, 'Peter Fulla' <pfulla@villageoflagrange.com>, 'Phil Kubisztal (D.C.)' <pkubisztal@lagrange.org>, 'Phil Lochirco' <plochirco@wsprings.com>, 'Phillip Grollo' <pgrollo@westchesterpolice.com>, 'R. Rodriguez' <rrodriguez@melroseparkpd.com>, 'Randy Buckner' <rbuckner@vil.bellwood.il.us>, 'Ray Holman' <ray_holman@cpr.ca>, 'Ray Leuser' <rleuser@indianheadpark-il.gov>, 'Rob Farenkopf' <rfarenkopf@wooddale.com>, 'Robert Anzaldi' <jrbpd1211@yahoo.com>, 'Robert Armony' <ramony@ci.berwyn.il.us>, 'Robert Klisz' <rklisz@elmwoodpark.org>, 'Robert Monaco' <rmonaco@ci.berwyn.il.us>, 'Robert Wardlaw' <rwardlaw@villageoflagrange.com>, 'Robert Wisch' <rwisch@burr-ridge.gov>, 'Ron Bongat' <bongat@oak-park.us>, 'Ron Miklas' <rmiklas@westchesterpolice.com>, 'Ron Murray (Dep. Chief)' <rmurray@wooddale.com>, 'Rose Moore' <sportyrose98@yahoo.com>, 'Ryan Husarik' <rhusarik@burr-ridge.gov>, 'Ryan O'Neil' <roneil@wooddale.com>, 'S. Pesce' <spesce@melroseparkpd.com>, 'SA Adam Hoogland' <adam.hoogland@ic.fbi.gov>, 'Sam Dorger' <jdorger@atg.state.il.us>, 'Sam Pitassi Jr.' <spitassijr@melroseparkpd.com>, 'Samir Patel' <samir.patel@usss.dhs.gov>, 'Sandro Scardamaglia' <sscardamaglia@ci.berwyn.il.us>, 'Scott Frey' <sfrey@forestpark.net>, 'Scott Warren' <swarren@oak-brook.org>, 'Sean Vazquez' <svazquez@northlakecity.com>, 'Shatonya Harris' <harriss@oak-park.us>, 'Shawn Witulski' <switulski@getipass.com>, 'Steve Abruzzo' <abruzzos@vil.bloomington.il.us>, 'Steve Mandat' <steve.mandat@elmhurst.org>, 'Steve Moody' <s Moody@cookcountygov.com>, 'Steve Pernice' <spernice@wooddale.com>, 'Steve Stopka' <sstopka@parkridgepolice.org>, 'T. O'Halloran (D.C.)' <TOHalloran@ci.berwyn.il.us>, 'Terrance Harris' <terrance.harris@va.gov>, 'Tim Carrol' <tcarrroll@river-forest.us>, 'Tim Mc Ewen'

<terrance.harris@va.gov>, 'Tim Carrol' <tcarroll@river-forest.us>, 'Tim Mc Ewen' <tmcewen@parkridgepolice.org>, 'Tim Roberts' <robertst@vil.bloomingtondale.il.us>, 'Tim Unzicker' <unzicker@oak-park.us>, 'Todd Kubish' <tkubish@vppd.org>, 'Todd Miller' <tmiller@hodgkinspd.org>, 'Tom Bojovic' <tbojovic@ci.berwyn.il.us>, 'Tom Burns' <burnst@vil.bloomingtondale.il.us>, 'Tom Ferris' <tferris@vofp.com>, Tom Fragakis <TFragakis@schillerparkil.us>, 'Tom Peterson' <riptidepiper@aol.com>, 'Tom Tate' <ttate@ci.berwyn.il.us>, 'Tony Cairra' <Peter.A.Cairra@cookcountyil.gov>, Trisha Vascik <trisha.vascik@elmhurst.org>, 'Vel Torlo' <vtorlo@oak-brook.org>, 'Vince Bruett' <bruettv@vil.bloomingtondale.il.us>, 'Vince LaManna' <vlamanna@westchesterpolice.com>, 'Wayne Holakovsky (Deputy Chief)' <wholakovsky@oakbrookterrace.net>, 'Wojciech Porebski' <wporebski@northlakecity.com>, 'Young Lee' <yylee@forestpark.net>, 'Zach Sienkiewicz' <z sienkiewicz@hillside-il.org>, DANIEL GROTH JR. (States Attorney) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DANIEL.GROTHJR>, Jason Moran (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Jason.moran>, KATE C GARCIA (States Attorney) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=KATE.OHARA>, Stephen Moody (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Stephen.moody>, Peter A Cairra (States Attorney) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Peter.A.Cairra>

Sent: May 8, 2015 3:52:36 PM CDT
Received: May 8, 2015 4:14:08 PM CDT
Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived Injustices 05082015.pdf

Det. William Martin
Schiller Park Police Dept.
9526 W. Irving Park Rd., Schiller Park, IL 60176.
(847) 671-8539 Direct
(847) 812-7875 Cell
(847) 671-9465 Fax

This electronic message transmission contains information from the Schiller Park Police Department that may be proprietary, confidential and/or privileged. The information is intended only for the use of the individual(s) or entity named above. If you are not the intended recipient, be aware that any disclosure, copying or distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender immediately by replying to the address listed in the "From:" field.

-----Original Message-----

From: Alana_Sorrentino@isp.state.il.us [mailto:Alana_Sorrentino@isp.state.il.us]
Sent: Friday, May 08, 2015 12:36 PM
To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Subject: (UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

Please see attached the Roll Call Release, "Criminal Hackers Target Police to Protest Perceived Injustices" dated May 8, 2015.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and cannot verify the contents to be factual. If you have any questions reference, this information, please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF

MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

Alana Sorrentino

Emergency Management Intelligence Officer | Statewide Terrorism & Intelligence Center

Liaison| Illinois Emergency Services Management Association (IESMA)

Western Illinois University | Illinois Terrorism Task Force

2200 South Dirksen Parkway, Springfield, IL 62703, Suite 238 Office Phone: 217-558-3739 | IESMA Phone: 217-557-4772

Email: Alana.Sorrentino@illinois.gov | Alana_Sorrentino@isp.state.il.us



ROLL CALL RELEASE

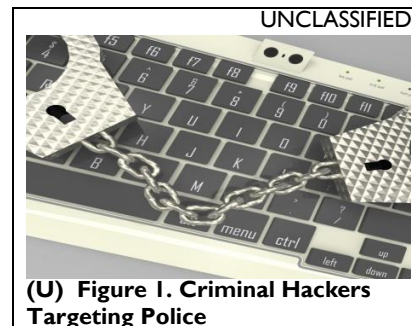
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:54 PM CDT
Received: May 8, 2015 12:57:43 PM CDT

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

From: Alana_Sorrentino@isp.state.il.us
To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:58 PM CDT
Received: May 8, 2015 1:06:31 PM CDT
Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived Injustices 05082015.pdf

Please see attached the Roll Call Release, "Criminal Hackers Target Police to Protest Perceived Injustices" dated May 8, 2015.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and cannot verify the contents to be factual. If you have any questions reference, this information, please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

Alana Sorrentino
Emergency Management Intelligence Officer | Statewide Terrorism & Intelligence Center
Liaison| Illinois Emergency Services Management Association (IESMA)
Western Illinois University | Illinois Terrorism Task Force
2200 South Dirksen Parkway, Springfield, IL 62703, Suite 238
Office Phone: 217-558-3739 | IESMA Phone: 217-557-4772
Email: Alana.Sorrentino@illinois.gov | Alana_Sorrentino@isp.state.il.us



ROLL CALL RELEASE

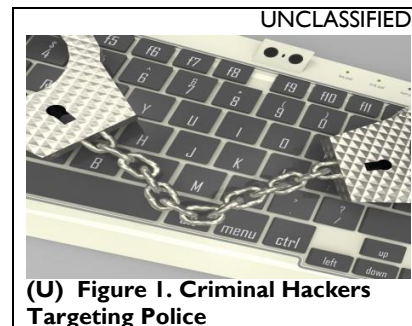
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:58 PM CDT
Received: May 8, 2015 1:06:32 PM CDT

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

From: Alana_Sorrentino@isp.state.il.us
To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:59 PM CDT
Received: May 8, 2015 1:07:21 PM CDT
Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived Injustices 05082015.pdf

Please see attached the Roll Call Release, "Criminal Hackers Target Police to Protest Perceived Injustices" dated May 8, 2015.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and cannot verify the contents to be factual. If you have any questions reference, this information, please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

Alana Sorrentino
Emergency Management Intelligence Officer | Statewide Terrorism & Intelligence Center
Liaison| Illinois Emergency Services Management Association (IESMA)
Western Illinois University | Illinois Terrorism Task Force
2200 South Dirksen Parkway, Springfield, IL 62703, Suite 238
Office Phone: 217-558-3739 | IESMA Phone: 217-557-4772
Email: Alana.Sorrentino@illinois.gov | Alana_Sorrentino@isp.state.il.us



ROLL CALL RELEASE

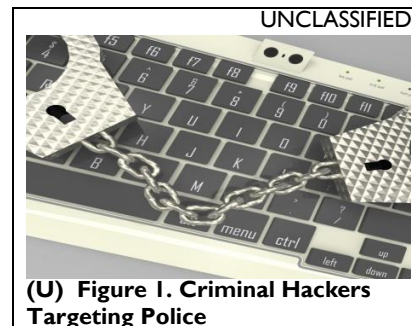
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:35:59 PM CDT
Received: May 8, 2015 1:07:21 PM CDT

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

From: Alana_Sorrentino@isp.state.il.us
To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:36:01 PM CDT
Received: May 8, 2015 12:58:10 PM CDT
Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived Injustices 05082015.pdf

Please see attached the Roll Call Release, "Criminal Hackers Target Police to Protest Perceived Injustices" dated May 8, 2015.

This intelligence information is being passed through as a courtesy to the originating agency. The STIC had no part in developing this information and cannot verify the contents to be factual. If you have any questions reference, this information, please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact STIC at 877-455-7842 if you have any questions or need additional information.

Alana Sorrentino
Emergency Management Intelligence Officer | Statewide Terrorism & Intelligence Center
Liaison| Illinois Emergency Services Management Association (IESMA)
Western Illinois University | Illinois Terrorism Task Force
2200 South Dirksen Parkway, Springfield, IL 62703, Suite 238
Office Phone: 217-558-3739 | IESMA Phone: 217-557-4772
Email: Alana.Sorrentino@illinois.gov | Alana_Sorrentino@isp.state.il.us



ROLL CALL RELEASE

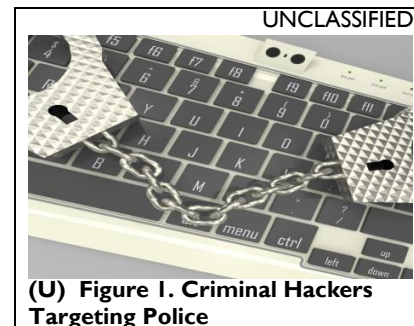
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014

(UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

To: donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 8, 2015 12:36:01 PM CDT
Received: May 8, 2015 12:58:15 PM CDT

FW: (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015

From: Daymon Johnston <djohnston@munster.org>
To: (pbmurray@nilea.com) <pbmurray@nilea.com>, Al Williamson (awilliamson@isp.in.gov) <awilliamson@isp.in.gov>, Alex Kenworthy (akenworthy@marionindiana.us) <akenworthy@marionindiana.us>, Andrew Paull (apaul@emichigancity.com) <apaul@emichigancity.com>, Brett Swanson (bswanson@lcsso.in.gov) <bswanson@lcsso.in.gov>, Brian Camadeca (bcamadeca@lakecountysheriff.com) <bcamadeca@lakecountysheriff.com>, cgootee@hammondpolice.com <cgootee@hammondpolice.com>, Chad Crosby (ccrosby@porterco-ps.org) <ccrosby@porterco-ps.org>, Chanto Iverson (Chanto_Iverson@isp.state.il.us) <Chanto_Iverson@isp.state.il.us>, Christopher Faigh (christopher.faigh@elkhartpolice.org) <christopher.faigh@elkhartpolice.org>, Corey McKinney (cmckinney@idoc.in.gov) <cmckinney@idoc.in.gov>, Cynthia Guest (cguest@co.st-joseph.in.us) <cguest@co.st-joseph.in.us>, Dave Hein (dpd22@aol.com) <dpd22@aol.com>, Dave Rybicki (drybicki@stjohnin.com) <drybicki@stjohnin.com>, David Veschak (David_Veschak@csx.com) <David_Veschak@csx.com>, Dion Campbell (dcampbell@emichigancity.com) <dcampbell@emichigancity.com>, Edward A. Rysiewicz (edward.rysiewicz@usdoj.gov) <edward.rysiewicz@usdoj.gov>, Eric Wiseman (ewiseman@porterco-ps.org) <ewiseman@porterco-ps.org>, Erik Holloway (eholloway@munster.org), Frank Diaz (juan.diaz@cookcountylil.gov) <juan.diaz@cookcountylil.gov>, Gene Hopkins (ghopkins@porterco-ps.org), J. R. Smith (jrsmith@doc.in.gov) <jrsmith@doc.in.gov>, Jake Zygmuntowski (jake_zygmuntowski@csx.com) <jake_zygmuntowski@csx.com>, James Donohue (jdonohue@merrillville.in.gov), Jamie Co (jcopollo@chestertonin.org) <jcopollo@chestertonin.org>, Jeffrey Cook (jcook@schererville.org) <jcook@schererville.org>, Jeremy Chavez (jdcpc67@yahoo.com) <jdcpc67@yahoo.com>, jharris@lakecountysheriff.com <jharris@lakecountysheriff.com>, John Cordova (jcordova@valpopd.com) <jcordova@valpopd.com>, John Eagan (jeagan@igc.in.gov) <jeagan@igc.in.gov>, Justine Pond (jpond@marion.k12.in.us) <jpond@marion.k12.in.us>, Karl Grimmer (karl_grimmer@csx.com) <karl_grimmer@csx.com>, Karl Hadayag (kmadayag@igc.in.gov) <kmadayag@igc.in.gov>, Karl Miller (Karl.miller@elkhartpolice.org) <Karl.miller@elkhartpolice.org>, Kenneth Forsythe (kforsythe@lc.hidta.net) <kforsythe@lc.hidta.net>, Kenneva Mapps (klmapps@idoc.in.gov) <klmapps@idoc.in.gov>, Kent Wilson (kwilson@marionindiana.us) <kwilson@marionindiana.us>, Kristopher Adams (krisadamslcpd@yahoo.com) <krisadamslcpd@yahoo.com>, Larry McKinley (slowmotion1378@comcast.net) <slowmotion1378@comcast.net>, Laura Lara (llara@igc.in.gov) <llara@igc.in.gov>, Lorena Butler (Lorena.Butler@cookcountylil.gov) <Lorena.Butler@cookcountylil.gov>, 'lthoma@milwaukee.gov' <lthoma@milwaukee.gov>, Marvin Giles (mgiles@idoc.in.gov) <mgiles@idoc.in.gov>, Michael Drohosky (mdrohosky@igc.in.gov) <mdrohosky@igc.in.gov>, Mike Cain (dpdmike@gmail.com) <dpdmike@gmail.com>, mschmidt@hammondpolice.com <mschmidt@hammondpolice.com>, Nathan Battleday (nbattleday@lcsso.in.gov) <nbattleday@lcsso.in.gov>, Nick Yoder (nyoder@co.adams.in.us) <nyoder@co.adams.in.us>, Patricia Yelkich (pay1254@sbcglobal.net) <pay1254@sbcglobal.net>, Patrick Quinn (patrick.quinn@chicagopolice.org) <patrick.quinn@chicagopolice.org>, pcicero@lcsso.in.gov <pcicero@lcsso.in.gov>, Raymond K. Humphrey (rhumphrey@isp.in.gov) <rhumphrey@isp.in.gov>, Richard Spicer (rspicer@valpopd.com) <rspicer@valpopd.com>, Sgt. Juan Beltran (juan.beltran@leo.gov) <juan.beltran@leo.gov>, Shawn O'Keefe (sokeefe@lakecountysheriff.com) <sokeefe@lakecountysheriff.com>, Stephen Bouffard (stephen.bouffard@cookcountylil.gov) <stephen.bouffard@cookcountylil.gov>, Steve Scheckel

<sscheckel@munster.org>, Tim Felver (tfelver@marionindiana.us)
<tfelver@marionindiana.us>, Timothy Shortt (tshortt@lcso.in.gov)
<tshortt@lcso.in.gov>, Tom Stinson (vstinson@idoc.in.gov)
<vstinson@idoc.in.gov>, Tyese Boone (tlboone@idoc.in.gov)
<tlboone@idoc.in.gov>, Watchcenter (Watchcenter@lc.hidta.net)
<Watchcenter@lc.hidta.net>, William Poling (wpoling@igc.in.gov)
<wpoling@igc.in.gov>, Brett Scheffel <bscheffel@munster.org>, Brian
Ayersman <bayersman@munster.org>, Brian Bernardino
<bbernardino@munster.org>, Brian Hernandez <bhernandez@munster.org>,
Bryan Oberc <boberc@munster.org>, Dan Broelmann
<dbroelmann@munster.org>, Daniel Croyle <dcroyle@munster.org>, David
Foulkes <dfoulkes@munster.org>, David Meyers <dmeyers@munster.org>,
Dean Miller <dmiller@munster.org>, Donald Lindemulder
<dlindemulder@munster.org>, Gabriel Isenblatter
<gisenblatter@munster.org>, Jack Deleeuw <jdeleeuw@munster.org>, James
Ghrist <jghrist@munster.org>, Joseph Newton <jnewton@munster.org>,
Joseph Pacheco <jpacheco@munster.org>, Joseph Wells
<jwells@munster.org>, Justin Goudreau <jgoudreau@munster.org>, Kevin
Cooley <kcooley@munster.org>, Mark Ashcraft <mashcraft@munster.org>,
Marshall Van Schouwen <mvanschouwen@munster.org>, Michael Silsby
<msilsby@munster.org>, Mike Janiga <mjaniga@munster.org>, Nathan
Martin <nmartin@munster.org>, Nolan Archer <narcher@munster.org>, Omar
Padilla <opadilla@munster.org>, Ryan Vassar <rvassar@munster.org>,
Spencer Lemmons <slemmons@munster.org>, Thomas Kuhlenschmidt
<tkuhlenschmidt@munster.org>, Tyler Niven <tniven@munster.org>, Juan
Diaz (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Juan.diaz>, Lorena Butler
(Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Lorenabutlera25>, Stephen
Bouffard (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Stephen.bouffard>,
(pbmurray@nilea.com)

Sent: May 8, 2015 12:48:26 PM CDT

Received: May 8, 2015 12:48:42 PM CDT

Attachments: (U--FOUO) RCR Criminal Hackers Target Police to Protest Perceived
Injust....pdf

From: Wiser, Jeffrey [mailto:jeffrey.wiser@HQ.DHS.GOV]

Sent: Friday, May 08, 2015 12:35 PM

Subject: (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015

(U//FOUO) The attached FOUO Roll Call Release (RCR) product was disseminated shortly ago regarding cyber threats to LE entities. Please feel free to share at the FOUO level within the State, local, and Federal LE communities. Thank you.

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

» (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.

» (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-

networking site containing the hashtag “#BlackLives Matter” announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.

» (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department’s website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department’s in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.

(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC’s “Guide to DDoS Attacks” for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and

complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of

reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies,

acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies

include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted

disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software

without the owner’s knowledge, instruction, or consent.

VR,

Jeffrey C. Wiser

DHS Office of Intelligence & Analysis (I&A)

Indiana Intelligence Fusion Center (IIFC)

317-234-4950 (Office)

317-408-8626 (Cell)



(U) Warning: This document is **UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

From: I&A_PB

Sent: Friday, May 08, 2015 1:06 PM

Cc: I&A_PB; Salinas, Lauren (CTR)

Subject: (U//FOUO) RCR: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015

(U//FOUO) This e-mail is a notification that the Roll Call Release: Criminal Hackers Target Police to Protest Perceived Injustices, dated 08 May 2015, has been posted to HSIN at

<https://hsin.dhs.gov> and will also be available via NCTC Current; the I&A websites on HSDN and HTSN (JWICS); and CapNet.

(U) **Intended Audience:** Federal, state, and local law enforcement officials; and the private sector

(U//FOUO) To locate the product on HSIN, go to HSIN Central page at <https://hsin.dhs.gov>, and copy and place the title in the search bar.

(U//FOUO) For more information regarding HSIN please visit http://www.dhs.gov/files/programs/gc_1156888108137.shtm or contact HSIN.Helpdesk@dhs.gov for access.

Very Respectfully,
I&A Intelligence Publications Division
Department of Homeland Security
IA.PM@hq.dhs.gov
(202) 282-8395
//lms//aeg//



ROLL CALL RELEASE

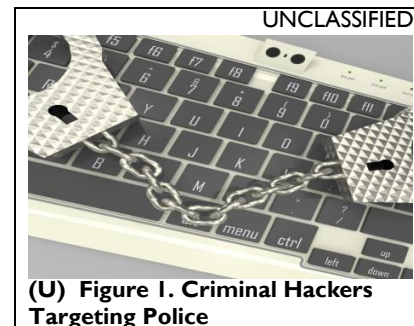
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014



ROLL CALL RELEASE

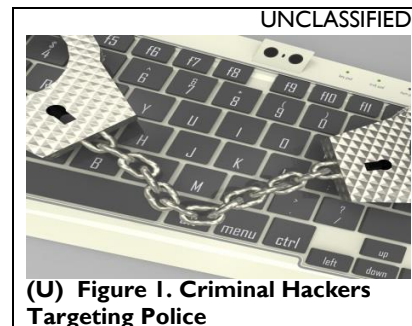
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag “#BlackLives Matter” announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's “Guide to DDoS Attacks” for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

Drive planning and preparedness efforts, training, and/or emergency response operations
Observe, identify, and/or disrupt threats
Share with partners
Allocate resources (e.g. equipment and personnel)
Reprioritize organizational focus
Author or adjust policies and guidelines

Initiate a law enforcement investigation
Initiate your own regional-specific analysis
Initiate your own topic-specific analysis
Develop long-term homeland security strategies
Do not plan to use
Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Request

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 29 October 2014

FW: (UFOUO) Criminal Hackers Target Police to Protest Perceived Injustices

To: 'Amy Kreml', 'Ann Montgomery', 'Anthony Garvey (Chief)', 'Anthony Gennett', 'Anthony Greco', 'Anthony Milazzo', 'Anthony Raitano', 'B Beck', 'Ben Kadolph', 'Bill Foster', 'Bill Frese', 'Bill Martin', 'Bill Stack', 'Bob Mance', 'Brad Mann', 'Brent Hoekstra', 'Brian Cantwell', 'Brian Dooley', 'Brian Greenenwald', 'Brian Strockis', 'Bruce Mason', 'Carlos Garcia', 'Carmelita Terry', 'Carol Dundovich', 'Charles Schauer', 'Chief Sam Pitassi', 'Chris Banaszynski', 'Chris Mowinski', 'Chris Pavini', 'Christopher Boenzi', 'Chuck Leuver', 'Cmndr Robert Nicholas', 'Corey O'Neal', 'Countryside Police Department', 'Curt Novak', 'D. Ransom', 'Damian Villagomez', 'Dan Albrecht', 'Dan Bresnahan', 'DANIEL GROTH JR. (States Attorney)', 'Daniel Haxton', 'Daniel Murphy', 'Daniel Pereda', 'Daniel Romanski', 'Dave Krull', 'Dave Rivkin', 'Dave Rohlicek', 'David Clark', 'David Green', 'David Kudla', 'David MacArtney', 'David Martin', 'Deborah Garcia', 'Dion Bobo', 'Dominic Panico', 'Don Batko', 'Ed Coughlin', 'Ed Rompa', 'Eric Katzin', 'Eric LoCoco', 'Erik Bernholdt', 'Fabian Navarro', 'Frank Cimaglia', 'Frank DeSimone', 'Frank Fagiano (Chief)', 'Frank Giammarese', 'Frank Homolka', 'Frank Lara', 'Frank Teutonico', 'Gary Pohanka', 'Gavin Zarbock', 'Genaro Manzo', 'George Zorzi', 'Gerald Karceski', 'Gil Espinosa', 'Giordano Manfredini', 'Greg Vesta', 'J. Drury (D.C.)', 'J. Nowacki', 'J.Schillinger', 'Jack Bridson', 'Jack Shannon', 'Jake Pollard', 'James Ferguson', 'James Lazansky', 'James Volpe', 'James Wagner', 'Jason Moran (Sheriff)', 'Jay Militello', 'Jeff Caldwell', 'Jeff Hill', 'Jeff Juan', 'Jeff Kucera', 'Jeff Sargent (Chief)', 'Jesus Ramos', 'Jim Greenwood', 'Jim Nowicki', 'Jim Ritz (Chief)', 'Jim Sasseti', 'Jim Schlicher', 'Jim Sperandio', 'Jimenez Allen', 'Jo Kujawinski', 'Jocelyn Ellis', 'Joe Duca', 'Joe Maranowicz', 'John Cairo', 'John Dörner', 'John Hadjioannou', 'John Helms', 'John Kerner', 'John Krueger', 'John Magnus', 'John Mudra', 'John Trevarthen', 'Joseph Green', 'Joseph Kanupke', 'Joseph Lukaszek', 'Joseph Riordan', 'Joseph Santangelo', 'Juan Duarte', 'Justin Patti', 'Karl Robinzine', 'KATE C GARCIA (States Attorney)', 'Kathy Shaughnessy (LT)', 'Ken Beres', 'Ken Gross', 'Ken Uher', 'Kenneth Howard', 'Kevin O'Connell', 'Kevin Susmarski', 'Kreg Floyd', 'Kris Gardner', 'L.Bartemio', 'LaGrange Park Detectives', 'Lane Niemann', 'Lee Zeitlin', 'Len Norek', 'Louis O'Rourke', 'M. Cimaglia (D.C.)', 'M.Winiarczyk', 'Marc Loftus', 'Mario Faso', 'Mario Valkov', 'Mark Altobella', 'Mark Astrella', 'Mark Battaglia', 'Mark Bozek', 'Mark Gallagher', 'Mark Van Stedum', 'Martin Milas', 'Mary Byrne', 'Melody Rissman', 'Melrose Park P.D.', 'Michael Barnes', 'Michael Castellano (Dep. Chief)', 'Michael Fellows', 'Michael Gaspari', 'Michael Hylton', 'Michael Keating', 'Michelle Glosky', 'Michelle Strugala', 'Mike Coughlin', 'Mike Jones', 'Mike Peters', 'Mike Rivas', 'Mike Scudiero', 'Neil Reyes', 'Nicholas Schiavone', 'Nick Petrovic', 'Ohara Johnson', 'P.Rocita', 'Patricia McConnell', 'Paul Finer', 'Paul Johnson', 'Paul Retzke', 'Pete Culafic', 'Pete Vizek', 'Peter Fulla', 'Phil Kubisztal (D.C.)', 'Phil Lochirco', 'Phillip Grollo', 'R.Rodriguez', 'Randy Buckner', 'Ray Holman', 'Ray Leuser', 'Rob Farenkopf', 'Robert Anzaldi', 'Robert Armony', 'Robert Klisz', 'Robert Monaco', 'Robert Wardlaw', 'Robert Wisch', 'Ron Bongat', 'Ron Miklas', 'Ron Murray (Dep. Chief)', 'Rose Moore', 'Ryan Husarik', 'Ryan O'Neil', 'S.Pesce', 'SA Adam Hoogland', 'Sam Dorger', 'Sam Pitassi Jr.', 'Samir Patel', 'Sandro Scardamaglia', 'Scott Frey', 'Scott Warren', 'Sean Vazquez', 'Shatonya Harris', 'Shawn Witulski', 'Steve Abruzzo', 'Steve Mandat', 'Stephen Moody (Sheriff)', 'Steve Pernice', 'Steve Stopka', 'T. O'Halloran (D.C.)', 'Terrance Harris', 'Tim Carroll', 'Tim McEwen', 'Tim Roberts', 'Tim Unzicker', 'Todd Kubish', 'Todd Miller', 'Tom Bojovic', 'Tom Burns', 'Tom Ferris', 'Tom Fragakis', 'Tom Peterson', 'Tom Tate', 'Peter A Cairra (States Attorney)', 'Trisha Vascik', 'Vel Torlo', 'Vince Bruett', 'Vince LaManna', 'Wayne Holakovsky (Deputy Chief)', 'Wojciech Porebski', 'Young Lee', 'Zach Sienkiewicz'

Sent: May 8, 2015 3:52:36 PM CDT

Received: May 8, 2015 4:14:10 PM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646420192@everbridge.net>
To: brenda.mckendrick@cookcountyil.gov
<brenda.mckendrick@cookcountyil.gov>, Brenda Mckendrick (Sheriff)
</O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Brenda.mckendrick>
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:53 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

**Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.**

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u>

	(13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646417852@everbridge.net>
To: john.konrad@cookcountyil.gov <john.konrad@cookcountyil.gov>, John Konrad (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=John.konrad>
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:52 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646420532@everbridge.net>
To: thomas.flemingjr@cookcountyil.gov <thomas.flemingjr@cookcountyil.gov>, Thomas Fleming Jr. (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Thomas.flemingjr>
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:50 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u>

	(13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646420602@everbridge.net>
To: steven.davis@cookcountyil.gov <steven.davis@cookcountyil.gov>, Steven Davis (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Steven.davis>
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:51 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game Ingress</u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: John Konrad (Sheriff), donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:52 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Steven Davis (Sheriff)
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:53 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Thomas Fleming Jr. (Sheriff)
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:50 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Brenda Mckendrick (Sheriff)
Sent: May 18, 2015 8:47:36 AM CDT
Received: May 18, 2015 8:47:54 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyl.gov <conf-646419692@everbridge.net>
To: john.blair@cookcountyl.gov <john.blair@cookcountyl.gov>, John Blair (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=John.blair>
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:47:50 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyl.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646421012@everbridge.net>
To: michael.boyce@cookcountyil.gov <michael.boyce@cookcountyil.gov>, Michael Boyce (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Michael.boyce>
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:47:53 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.
Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646418532@everbridge.net>
To: martin.bennett@cookcountyil.gov <martin.bennett@cookcountyil.gov>, Martin Bennett (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Martin.bennett>
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:48:00 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

[\(U//FOUO\) Use of Unidentified Machine to Alter US Government Checks, as of April 2015](#)
(14 May 2015)

[\(U//FOUO\) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015](#)
(14 May 2015)

[\(U//FOUO\) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot](#)
(13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) “Muhammad Art Exhibit & Contest” in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to “e-Enabled” Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: John Blair (Sheriff), donotreply@isp.state.il.us
Cc: Cyber_Security@isp.state.il.us
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:47:51 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Michael Boyce (Sheriff)
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:47:56 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Martin Bennett (Sheriff)
Sent: May 18, 2015 8:47:37 AM CDT
Received: May 18, 2015 8:48:00 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646422172@everbridge.net>
To: gilberto.guerrero@cookcountyil.gov <gilberto.guerrero@cookcountyil.gov>, Gilberto Guerrero (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Gilberto.guerrero>
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:52 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyiil.gov <conf-646418282@everbridge.net>
To: kevin.ruel@cookcountyiil.gov <kevin.ruel@cookcountyiil.gov>, Kevin Ruel (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Kevin.ruel>
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:52 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyiil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.
Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyil.gov <conf-646419972@everbridge.net>
To: helen.burke@cookcountyil.gov <helen.burke@cookcountyil.gov>, Helen Burke (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Helen.burke>
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:55 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

	<u>(U//FOUO) Use of Unidentified Machine to Alter US Government Checks, as of April 2015</u> (14 May 2015)
	<u>(U//FOUO) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015</u> (14 May 2015)
	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.
Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game Ingress</u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015

No. 02

LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game Ingress</u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Gilberto Guerrero (Sheriff)
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:53 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Kevin Ruel (Sheriff)
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:52 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Helen Burke (Sheriff)
Sent: May 18, 2015 8:47:38 AM CDT
Received: May 18, 2015 8:47:56 AM CDT

DHSEM SAU 01 LEO 18May2015 FBI Intel

From: duty.desk@cookcountyl.gov <conf-646419782@everbridge.net>
To: keith.formell@cookcountyl.gov <keith.formell@cookcountyl.gov>, Keith Formell (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Keithformellbe3>
Sent: May 18, 2015 8:47:40 AM CDT
Received: May 18, 2015 8:47:59 AM CDT
Attachments: DHSEM+01+SAU+02+LEO+FBI+Intel.pdf

Date: 18 May 2015

No. 01

RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyl.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement
Enterprise Portal

Homeland Security
Information Network

Regional Information
Sharing Systems

Open Source

[\(U//FOUO\) Use of Unidentified Machine to Alter US Government Checks, as of April 2015](#)
(14 May 2015)

[\(U//FOUO\) Multiple Bank Robberies Occurring in the Chicago Area as of May 2015](#)
(14 May 2015)

[\(U//FOUO\) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot](#)
(13 May 2015)

	<u>(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot</u> (13 May 2015)
	<u>(U//FOUO) National Biosurveillance Integration Center – The Ebola Virus Disease in West Africa</u> (12 May 2015)
	<u>(U//FOUO) Bulk Cash Smuggling Center C-Note</u> (11 May 2015)
	<u>(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices</u> (08 May 2015)
	<u>(U//LES) Violence Possible at Kansas City, Missouri Somaliland Independence Day Celebration on May 16, 2015</u> (08 May 2015)
	<u>(U//LES) Identification of Alleged Distribution Point for Synthetic Marijuana Oil in Hammond, Indiana, as of March 2015</u> (08 May 2015)
	<u>(U//FOUO) Traffickers Exploit Unregulated Ownership of Land in Apure, Venezuela</u> (08 May 2015)
	<u>(U//FOUO) Second Quarter UAC Migration Indicators Suggest Third Quarter Levels Below FY 2014 Surge</u> (08 May 2015)

Federal Bureau of Investigation
Central Region Intelligence Integration
IA, IL, IN, KS, MI, MO, NE, WI
Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924 , 793, 798, 952, and 192

JH/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

- 2. The holder of the information will comply with access and dissemination restrictions.
- 3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0800	2.0802
--------	--------

If you have any questions, please e-mail: duty.desk@cookcountyil.gov



SAU

SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 01 May 2015
No. 02
LEO

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail:
DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.



UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE

EMAIL INFORMATION





















Recent / Relevant Reporting

Please send links of products for inclusion in this email to the contact email address at the bottom of this communication.

SYSTEM ICONS FOR PRODUCT LINK ACCESS

Law Enforcement Enterprise Portal	Homeland Security Information Network	Regional Information Sharing Systems	Open Source
			

	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//FOUO) "Muhammad Art Exhibit & Contest" in Texas on 03 May Likely to Prompt Violent Extremist Reaction Abroad; Violence Less Likely at Home</u> (30 April 2015)
	<u>(U//LES) Receipt of Envelopes Containing Threatening Letters and Non-Hazardous Substances to Five Chicago, Illinois-Area Locations, as of 28 April 2015</u> (30 April 2015)
	<u>(U//FOUO) NCTC Counterterrorism Weekly</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Anarchist Extremists Likely to Exploit 01 May Events for Violent Activity</u> (28 April 2015)
	<u>(U//FOUO) Proposed Changes to Real Estate Disclosure Forms May Negatively Impact Law Enforcement Efforts to Combat Mortgage Fraud, as of August 2015</u> (28 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Vulnerabilities and Threats to "e-Enabled" Aircraft Avionics and Other Systems</u> (24 April 2015)
	<u>(U//FOUO) Corrupt Clearing Firms Are Likely Collaborating with Corrupt Brokerages to Facilitate Precious Metals Investment Fraud</u> (24 April 2015)
	<u>(U//FOUO) Identification of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)

	<u>(U//FOUO) Structure of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Activity of Hispanic Gang, Corona 13, in Topeka and Emporia, Kansas, as of March 2015</u> (24 April 2015)
	<u>(U//FOUO) Homemade Explosives Information Bulletin</u> (24 April 2015)
	<u>(U//LES) Potential Increase in Suspicious Activity Reporting as a Result of Participation in the Mobile Device Game <i>Ingress</i></u> (20 April 2015)
	<u>(U//LES) GPS Tracking Devices Utilized by Drug Trafficking Organizations</u> (20 April 2015)
<div style="text-align: center;">   </div> <div style="text-align: center; background-color: #003366; color: white; padding: 5px; margin-top: 10px;"> UNCLASSIFIED // LAW ENFORCEMENT SENSITIVE </div>	

Federal Bureau of Investigation
 Central Region Intelligence Integration
 IA, IL, IN, KS, MI, MO, NE, WI
 Office Location: Chicago, IL 60608
CENTRAL_REGION_INTEGRATION@ic.fbi.gov

Law Enforcement Online (LEO) -- https://leo.cjis.gov/webcenter/spaces/c_regint/home

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE// The attached provides law enforcement with current, relevant information developed from on-going investigations and analysis.

SECURITY NOTE: The information contained is classified "Law Enforcement Sensitive". No portion of this document should be released to the media or general public. Any release of this information could adversely affect or jeopardize investigative activities. Furthermore - All classified information is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of classified information may constitute a violation of Title 18, sections 641, 793, 798, 952, and 1924, 793, 798, 952, and 192

BT/ML

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- 1.** FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- 2.** The holder of the information will comply with access and dissemination restrictions.
- 3.** Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

DHSEM SAU 01 LEO 18May2015 FBI Intel

To: Keith Formell (Sheriff)
Sent: May 18, 2015 8:47:40 AM CDT
Received: May 18, 2015 8:48:02 AM CDT

FW: Weekly Bulletin

From: Daymon Johnston <djohnston@munster.org>
To: (pbmurray@nilea.com) <pbmurray@nilea.com>, Al Williamson
(awilliamson@isp.in.gov) <awilliamson@isp.in.gov>, Alex Kenworthy
(akenworthy@marionindiana.us) <akenworthy@marionindiana.us>, Andrew
Paull (apaul@emichigancity.com) <apaul@emichigancity.com>, Brett
Swanson (bswanson@lcsso.in.gov) <bswanson@lcsso.in.gov>, Brian
Camadeca (bcamadeca@lakecountysheriff.com)
<bcamadeca@lakecountysheriff.com>, cgootee@hammondpolice.com
<cgootee@hammondpolice.com>, Chad Crosby (ccrosby@porterco-ps.org)
<ccrosby@porterco-ps.org>, Chanto Iverson (Chanto_Iverson@isp.state.il.us)
<Chanto_Iverson@isp.state.il.us>, Christopher Faigh
(christopher.faigh@elkhartpolice.org) <christopher.faigh@elkhartpolice.org>,
Corey McKinney (cmckinney@idoc.in.gov) <cmckinney@idoc.in.gov>, Cynthia
Guest (cguest@co.st-joseph.in.us) <cguest@co.st-joseph.in.us>, Dave Hein
(dpd22@aol.com) <dpd22@aol.com>, Dave Rybicki (drybicki@stjohnin.com)
<drybicki@stjohnin.com>, David Veschak (David_Veschak@csx.com)
<David_Veschak@csx.com>, Dion Campbell (dcampbell@emichigancity.com)
<dcampbell@emichigancity.com>, Edward A. Rysiewicz
(edward.rysiewicz@usdoj.gov) <edward.rysiewicz@usdoj.gov>, Eric Wiseman
(ewiseman@porterco-ps.org) <ewiseman@porterco-ps.org>, Erik Holloway
<eholloway@munster.org>, Frank Diaz (juan.diaz@cookcountylil.gov)
<juan.diaz@cookcountylil.gov>, Gene Hopkins (ghopkins@porterco-ps.org),
J. R. Smith (jrsmith@doc.in.gov) <jrsmith@doc.in.gov>, Jake Zygmuntowski
(jake_zygmuntowski@csx.com) <jake_zygmuntowski@csx.com>, James
Donohue <jdonohue@merrillville.in.gov>, Jamie Co
(jcopollo@chestertonin.org) <jcopollo@chestertonin.org>, Jeffrey Cook
(jcook@scherville.org) <jcook@scherville.org>, Jeremy Chavez
(jdcpc67@yahoo.com) <jdcpc67@yahoo.com>, jharris@lakecountysheriff.com
<jharris@lakecountysheriff.com>, John Cordova (jcordova@valpopd.com)
<jcordova@valpopd.com>, John Eagan (jeagan@igc.in.gov)
<jeagan@igc.in.gov>, Justine Pond (jpond@marion.k12.in.us)
<jpond@marion.k12.in.us>, Karl Grimmer (karl_grimmer@csx.com)
<karl_grimmer@csx.com>, Karl Hadayag (kmadayag@igc.in.gov)
<kmadayag@igc.in.gov>, Karl Miller (Karl.miller@elkhartpolice.org)
<Karl.miller@elkhartpolice.org>, Kenneth Forsythe (kforsythe@lc.hidta.net)
<kforsythe@lc.hidta.net>, Kenneva Mapps (klmapps@idoc.in.gov)
<klmapps@idoc.in.gov>, Kent Wilson (kwilson@marionindiana.us)
<kwilson@marionindiana.us>, Kristopher Adams (krisadamslcpd@yahoo.com)
<krisadamslcpd@yahoo.com>, Larry McKinley
(slowmotion1378@comcast.net) <slowmotion1378@comcast.net>, Laura Lara
(llara@igc.in.gov) <llara@igc.in.gov>, Lorena Butler
(Lorena.Butler@cookcountylil.gov) <Lorena.Butler@cookcountylil.gov>,
'lthoma@milwaukee.gov' <lthoma@milwaukee.gov>, Marvin Giles
(mgiles@idoc.in.gov) <mgiles@idoc.in.gov>, Michael Drohosky
(mdrohosky@igc.in.gov) <mdrohosky@igc.in.gov>, Mike Cain
(dpdmike@gmail.com) <dpdmike@gmail.com>,
mschmidt@hammondpolice.com <mschmidt@hammondpolice.com>, Nathan
Battleday (nbattleday@lcsso.in.gov) <nbattleday@lcsso.in.gov>, Nick Yoder
(nyoder@co.adams.in.us) <nyoder@co.adams.in.us>, Patricia Yelkich
(pay1254@sbcglobal.net) <pay1254@sbcglobal.net>, Patrick Quinn
(patrick.quinn@chicagopolice.org) <patrick.quinn@chicagopolice.org>,
pcicero@lcsso.in.gov <pcicero@lcsso.in.gov>, Raymond K. Humphrey
(rhumphrey@isp.in.gov) <rhumphrey@isp.in.gov>, Richard Spicer
(rspicer@valpopd.com) <rspicer@valpopd.com>, Sgt. Juan Beltran
(juan.beltran@leo.gov) <juan.beltran@leo.gov>, Shawn O'Keefe
(sokeefe@lakecountysheriff.com) <sokeefe@lakecountysheriff.com>, Stephen
Bouffard (stephen.bouffard@cookcountylil.gov)
<stephen.bouffard@cookcountylil.gov>, Steve Scheckel
<sscheckel@munster.org>, Tim Felver (tfelver@marionindiana.us)
<tfelver@marionindiana.us>, Timothy Shortt (tshortt@lcsso.in.gov)

<tshortt@lcso.in.gov>, Tom Stinson (vstinson@idoc.in.gov)
<vstinson@idoc.in.gov>, Tyese Boone (tlboone@idoc.in.gov)
<tlboone@idoc.in.gov>, Watchcenter (Watchcenter@lc.hidta.net)
<Watchcenter@lc.hidta.net>, William Poling (wpoling@igc.in.gov)
<wpoling@igc.in.gov>, Brett Scheffel <bscheffel@munster.org>, Brian
Ayersman <bayersman@munster.org>, Brian Bernardino
<bbernardino@munster.org>, Brian Hernandez <bhernandez@munster.org>,
Bryan Oberc <boberc@munster.org>, Dan Broelmann
<dbroelmann@munster.org>, Daniel Croyle <dcroyle@munster.org>, David
Foulkes <dfoulkes@munster.org>, David Meyers <dmeyers@munster.org>,
Dean Miller <dmiller@munster.org>, Donald Lindemulder
<dlindemulder@munster.org>, Gabriel Isenblatter
<gisenblatter@munster.org>, Jack Deleeuw <jdeleeuw@munster.org>, James
Ghrist <jghrist@munster.org>, Joseph Newton <jnewton@munster.org>,
Joseph Pacheco <jpacheco@munster.org>, Joseph Wells
<jwells@munster.org>, Justin Goudreau <jgoudreau@munster.org>, Kevin
Cooley <kcooley@munster.org>, Mark Ashcraft <mashcraft@munster.org>,
Marshall Van Schouwen <mvanschouwen@munster.org>, Michael Silsby
<msilsby@munster.org>, Mike Janiga <mjaniga@munster.org>, Nathan
Martin <nmartin@munster.org>, Nolan Archer <narcher@munster.org>, Omar
Padilla <opadilla@munster.org>, Ryan Vassar <rvassar@munster.org>,
Spencer Lemmons <slemmons@munster.org>, Thomas Kuhlenschmidt
<tkuhlenschmidt@munster.org>, Tyler Niven <tniven@munster.org>, Juan
Diaz (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Juan.diaz>, Lorena Butler
(Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Lorenabutlera25>, Stephen
Bouffard (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Stephen.bouffard>,
(pbmurray@nilea.com)

Sent: May 22, 2015 9:53:46 AM CDT
Received: May 22, 2015 9:54:13 AM CDT
Attachments: 2015_05_21 Weekly Bulletin.pdf

From: Rose, Danny L. [mailto:drose@iifc.IN.gov]
Sent: Thursday, May 21, 2015 9:06 PM
To: IIFC
Subject: Weekly Bulletin

Attached.

Stay Safe!

DISCLAIMER: Any information supplied to you is **LEAD INFORMATION ONLY**. The contents **CAN NOT** be placed in any law enforcement report, probable cause affidavit, court proceeding, or any document that may become public. Contact the IIFC for further clarification and/or guidance for proper dissemination.

This correspondence is the property of the Indiana Intelligence Fusion Center and is intended for the addressed recipients only. Any unauthorized use or distribution is prohibited. Your cooperation is appreciated.

Dan Rose
Deputy Director of Intelligence and Analysis
Indiana Intelligence Fusion Center
email: drose@iifc.IN.gov
danny.rose@leo.gov
Work Line: 317 234-4683
Verizon Cell: 317 691-5042

FW: Weekly Bulletin

From: Lorena Butler (Sheriff) <Lorena.Butler@cookcountyil.gov>, Lorena Butler (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=LORENABUTLERA25>
To: Brian Duffy (Sheriff) <Brian.Duffy@cookcountyil.gov>, Brian Duffy (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Brianduffy65>
Sent: May 22, 2015 10:11:52 AM CDT
Received: May 22, 2015 10:11:53 AM CDT
Attachments: 2015_05_21 Weekly Bulletin.pdf

Lorena Butler
Intelligence Analyst
Cook County Sheriff's Police Department
Sheriff's Office Intelligence Center (SOIC)
Work: (773) 674-3519
Email: Lorena.Butler@cookcountyil.gov

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

From: Daymon Johnston [mailto:djohnston@munster.org]
Sent: Friday, May 22, 2015 9:54 AM
To: (pbmurray@nilea.com); Al Williamson (awilliamson@isp.in.gov); Alex Kenworthy (akenworthy@marionindiana.us); Andrew Paull (apaull@emichigancity.com); Brett Swanson (bswanson@lcsso.in.gov); Brian Camadeca (bcamadeca@lakecountysheriff.com); cgootee@hammondpolice.com; Chad Crosby (ccrosby@porterco-ps.org); Chanto Iverson (Chanto_Iverson@isp.state.il.us); Christopher Faigh (christopher.faigh@elkhartpolice.org); Corey McKinney (cmckinney@idoc.in.gov); Cynthia Guest (cguest@co.st-joseph.in.us); Dave Hein (dpd22@aol.com); Dave Rybicki (drybicki@stjohnin.com); David Veschak (David_Veschak@csx.com); Dion Campbell (dcampbell@emichigancity.com); Edward A. Rysiewicz (edward.rysiewicz@usdoj.gov); Eric Wiseman (ewiseman@porterco-ps.org); Erik Holloway; Juan Diaz (Sheriff); Gene Hopkins; J. R. Smith (jrsmith@doc.in.gov); Jake Zygmuntowski (jake_zygmuntowski@csx.com); James Donohue; Jamie Co (jcopollo@chestertonin.org); Jeffrey Cook (jcook@schererville.org); Jeremy Chavez (jdcpc67@yahoo.com); jharris@lakecountysheriff.com; John Cordova (jcordova@valpopd.com); John Eagan (jeagan@igc.in.gov); Justine Pond (jpond@marion.k12.in.us); Karl Grimmer (karl_grimmer@csx.com); Karl Hadayag (kmadayag@igc.in.gov); Karl Miller (Karl.miller@elkhartpolice.org); Kenneth Forsythe (kforsythe@lc.hidta.net); Kenneva Mapps (klmapps@idoc.in.gov); Kent Wilson (kwilson@marionindiana.us); Kristopher Adams (krisadamslcpd@yahoo.com); Larry McKinley (slowmotion1378@comcast.net); Laura Lara (llara@igc.in.gov); Lorena Butler (Sheriff); 'lthoma@milwaukee.gov'; Marvin Giles (mgiles@idoc.in.gov); Michael Drohosky (mdrohosky@igc.in.gov); Mike Cain (dpdmike@gmail.com); mschmidt@hammondpolice.com; Nathan Battleday (nbattleday@lcsso.in.gov); Nick Yoder (nyoder@co.adams.in.us); Patricia Yelkich (pay1254@sbcglobal.net); Patrick Quinn (patrick.quinn@chicagopolice.org); pcicero@lcsso.in.gov; Raymond K. Humphrey (rhumphrey@isp.in.gov); Richard Spicer (rspicer@valpopd.com); Sgt. Juan Beltran (juan.beltran@leo.gov); Shawn O'Keefe (sokeefe@lakecountysheriff.com); Stephen Bouffard (Sheriff); Steve Scheckel; Tim Felter (tfelter@marionindiana.us); Timothy Shortt (tshortt@lcsso.in.gov); Tom Stinson (vstinson@idoc.in.gov); Tyese Boone (tlboone@idoc.in.gov); Watchcenter (Watchcenter@lc.hidta.net); William Poling (wpoling@igc.in.gov); Brett Scheffel; Brian Ayersman; Brian

Bernardino; Brian Hernandez; Bryan Oberc; Dan Broelmann; Daniel Croyle; David Foulkes; David Meyers; Dean Miller; Donald Lindemulder; Gabriel Isenblatter; Jack Deleeuw; James Ghrist; Joseph Newton; Joseph Pacheco; Joseph Wells; Justin Goudreau; Kevin Cooley; Mark Ashcraft; Marshall Van Schouwen; Michael Silsby; Mike Janiga; Nathan Martin; Nolan Archer; Omar Padilla; Ryan Vassar; Spencer Lemmons; Thomas Kuhlenschmidt; Tyler Niven
Subject: FW: Weekly Bulletin

From: Rose, Danny L. [mailto:drose@iifc.IN.gov]
Sent: Thursday, May 21, 2015 9:06 PM
To: IIFC
Subject: Weekly Bulletin

Attached.

Stay Safe!

DISCLAIMER: Any information supplied to you is **LEAD INFORMATION ONLY**. The contents **CAN NOT** be placed in any law enforcement report, probable cause affidavit, court proceeding, or any document that may become public. Contact the IIFC for further clarification and/or guidance for proper dissemination.

This correspondence is the property of the Indiana Intelligence Fusion Center and is intended for the addressed recipients only. Any unauthorized use or distribution is prohibited. Your cooperation is appreciated.

Dan Rose
Deputy Director of Intelligence and Analysis
Indiana Intelligence Fusion Center
email: drose@iifc.IN.gov
danny.rose@leo.gov
Work Line: 317 234-4683
Verizon Cell: 317 691-5042

FW: Weekly Bulletin

From: Lorena Butler (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=LORENABUTLERA25>
To: Brian Duffy (Sheriff) </O=CCBOT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Brianduffyf65>
Sent: May 22, 2015 10:11:52 AM CDT
Received: May 22, 2015 10:11:00 AM CDT
Attachments: 2015_05_21 Weekly Bulletin.pdf

Lorena Butler
Intelligence Analyst
Cook County Sheriff's Police Department
Sheriff's Office Intelligence Center (SOIC)
Work: (773) 674-3519
Email: Lorena.Butler@cookcountyil.gov

THIS IS A CONFIDENTIAL LAW ENFORCEMENT COMMUNICATION. The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute, transmit or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action relative to the information contained in this communication and/or attachments. This e-mail and any attached documents may contain Law Enforcement Sensitive material and should not be disseminated outside of official law enforcement channels. The information contained in this message as well as any attachments shall not be released to the media or the general public.

From: Daymon Johnston [mailto:djohnston@munster.org]
Sent: Friday, May 22, 2015 9:54 AM
To: (pbmurray@nilea.com); Al Williamson (awilliamson@isp.in.gov); Alex Kenworthy (akenworthy@marionindiana.us); Andrew Paull (apaull@emichigancity.com); Brett Swanson (bswanson@lcsso.in.gov); Brian Camadeca (bcamadeca@lakecountysheriff.com); cgootee@hammondpolice.com; Chad Crosby (ccrosby@porterco-ps.org); Chanto Iverson (Chanto_Iverson@isp.state.il.us); Christopher Faigh (christopher.faigh@elkhartpolice.org); Corey McKinney (cmckinney@idoc.in.gov); Cynthia Guest (cguest@co.st-joseph.in.us); Dave Hein (dpd22@aol.com); Dave Rybicki (drybicki@stjohnin.com); David Veschak (David_Veschak@csx.com); Dion Campbell (dcampbell@emichigancity.com); Edward A. Rysiewicz (edward.rysiewicz@usdoj.gov); Eric Wiseman (ewiseman@porterco-ps.org); Erik Holloway; Juan Diaz (Sheriff); Gene Hopkins; J. R. Smith (jrsmith@doc.in.gov); Jake Zygmuntowski (jake_zygmuntowski@csx.com); James Donohue; Jamie Co (jcopollo@chestertonin.org); Jeffrey Cook (jcook@schererville.org); Jeremy Chavez (jdcpc67@yahoo.com); jharris@lakecountysheriff.com; John Cordova (jcordova@valpopd.com); John Eagan (jeagan@igc.in.gov); Justine Pond (jpond@marion.k12.in.us); Karl Grimmer (karl_grimmer@csx.com); Karl Hadayag (kmadayag@igc.in.gov); Karl Miller (Karl.miller@elkhartpolice.org); Kenneth Forsythe (kforsythe@lc.hidta.net); Kenneva Mapps (klmapps@idoc.in.gov); Kent Wilson (kwilson@marionindiana.us); Kristopher Adams (krisadamslcpd@yahoo.com); Larry McKinley (slowmotion1378@comcast.net); Laura Lara (llara@igc.in.gov); Lorena Butler (Sheriff); 'lthoma@milwaukee.gov'; Marvin Giles (mgiles@idoc.in.gov); Michael Drohosky (mdrohosky@igc.in.gov); Mike Cain (dpdmike@gmail.com); mschmidt@hammondpolice.com; Nathan Battleday (nbattleday@lcsso.in.gov); Nick Yoder (nyoder@co.adams.in.us); Patricia Yelkich (pay1254@sbcglobal.net); Patrick Quinn (patrick.quinn@chicagopolice.org); pcicero@lcsso.in.gov; Raymond K. Humphrey (rhumphrey@isp.in.gov); Richard Spicer (rspicer@valpopd.com); Sgt. Juan Beltran (juan.beltran@leo.gov); Shawn O'Keefe (sokeefe@lakecountysheriff.com); Stephen Bouffard (Sheriff); Steve Scheckel; Tim Felver (tfelver@marionindiana.us); Timothy Shortt (tshortt@lcsso.in.gov); Tom Stinson (vstinson@idoc.in.gov); Tyese Boone (tlboone@idoc.in.gov); Watchcenter (Watchcenter@lc.hidta.net); William Poling (wpoling@igc.in.gov); Brett Scheffel; Brian Ayersman; Brian Bernardino; Brian Hernandez; Bryan Oberc; Dan Broelmann; Daniel Croyle; David Foulkes; David Meyers; Dean Miller;

Donald Lindemulder; Gabriel Isenblatter; Jack Deleeuw; James Ghrist; Joseph Newton; Joseph Pacheco; Joseph Wells; Justin Goudreau; Kevin Cooley; Mark Ashcraft; Marshall Van Schouwen; Michael Silsby; Mike Janiga; Nathan Martin; Nolan Archer; Omar Padilla; Ryan Vassar; Spencer Lemmons; Thomas Kuhlenschmidt; Tyler Niven
Subject: FW: Weekly Bulletin

From: Rose, Danny L. [mailto:drose@iifc.IN.gov]
Sent: Thursday, May 21, 2015 9:06 PM
To: IIFC
Subject: Weekly Bulletin

Attached.

Stay Safe!

DISCLAIMER: Any information supplied to you is **LEAD INFORMATION ONLY**. The contents **CAN NOT** be placed in any law enforcement report, probable cause affidavit, court proceeding, or any document that may become public. Contact the IIFC for further clarification and/or guidance for proper dissemination.

This correspondence is the property of the Indiana Intelligence Fusion Center and is intended for the addressed recipients only. Any unauthorized use or distribution is prohibited. Your cooperation is appreciated.

Dan Rose
Deputy Director of Intelligence and Analysis
Indiana Intelligence Fusion Center
email: drose@iifc.IN.gov
danny.rose@leo.gov
Work Line: 317 234-4683
Verizon Cell: 317 691-5042



INDIANA INTELLIGENCE FUSION CENTER

302 W. Washington St. Room E-243, Indianapolis, IN 46201

Phone: 866-400-4432; Fax: 317-234-4749

Email: iifc@iifc.in.gov

Intelligence Bulletin

21 May 2015

Information Cutoff Date –21 May 2015

INSIDE THIS BULLETIN:

- Officer Awareness: President Obama Signs National Blue Alert Act—P. 2
- RFI: Edinburgh (IN) PD Seeking Agencies with Info. on Recovered Semi-Tractor Filter—P. 2-3
- RFI: Carmel (IN) PD Seeking Theft Suspects—P. 3
- Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Govt Targeting—P. 3-4
- Select Federal Products/Reports Recently Released—P. 4-5
- STATE—INGangNetwork —P. 6-7
- CUSTOMER SATISFACTION SURVEY— P. 8

UPCOMING SIGNIFICANT EVENTS/DATES:

23 May 2015: 500 Festival Parade—Indianapolis, IN

24 May 2015: Indianapolis 500—Speedway, IN

****** If your agency knows of any upcoming events where large crowds are expected and would like them included in the bulletin for awareness purposes, please email information to iifc@iifc.in.gov with the subject line WEEKLY INTELLIGENCE BULLETIN. ******

PN59976

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

Officer Awareness: President Obama Signs National Blue Alert Act

(U) President Barack OBAMA has signed into law a measure to create a nationwide alert system to help catch anyone who injures, kills, or who has made an imminent or credible threat to cause serious injury or death to a law enforcement officer.

(U) The new system would be similar to the Amber Alerts used to find abducted children.

(U) The bill is named for New York City police officers Rafael RAMOS and Wenjian LIU, who were shot and killed in Brooklyn, NY days before Christmas in 2014 by a man who later killed himself. The killer posted threats to law enforcement on social media before the attack. Implementing a nationwide Blue Alert system will help to ensure that information on credible threats, like those posted by the individual who killed detectives RAMOS and LIU, is widely disseminated so that officers have advanced warning, and can apprehend the criminal before he or she can do more harm.

(U) The bill was so uncontroversial that it passed both the House and the Senate by voice vote.

Source: bluealert.us; www.policeone.com

RFI: Edinburgh (IN) Police Department Seeking Agencies with Information on Recovered Semi-Tractor Filter

(U//LES) The Edinburgh (IN) Police Department is seeking agencies that may have information on the semi-tractor filter pictured below that was recovered during a traffic arrest that occurred on 15 May 2015 in Edinburgh, IN. The suspect that was arrested thought the filter was a catalytic converter.



This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//LES) Any agency with thefts possibly connected to the above pictured filter should contact Det. Robert CROCKER; Edinburgh Police Department; 812-526-2636 or rcrocker@edinburgh.in.us.

Source: Edinburgh Police Department

RFI: Carmel (IN) Police Department Seeking Theft Suspects

(U//LES) The Carmel (IN) Police Department is seeking the three suspects pictured below in reference to a theft investigation. The three suspects worked together to commit a short change scam that occurred on 28 April 2015 at a Village Pantry convenience store located in Carmel, IN.

(U//LES) The first suspect entered the store, made a small purchase, and left. The second suspect then entered and proceeded to the register where he began an unknown transaction. The third suspect then distracted an employee at the checkout area. The first suspect returned and made a drink at the fountain machine. He then dropped the drink causing the store manager to walk over and clean up the spill. The second suspect then completed a short change theft at the register by confusing the remaining clerk.



(U//LES) Any agency with similar incidents or similar suspects should contact Det. T. MCINTYRE; Carmel Police Department; 317-571-2728 or tmcintyre@carmel.in.gov.

Source: Carmel Police Department

Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Government Targeting

(U//LES) On 16 May 2015 actors associated with Vikingdom posted a warning on Twitter stating that "U.S. websites are going to be under a massive ddos attack so watch out!" This warning was followed by

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

a post early on 18 May 2015 using the hashtag "#DominateAmerica." CIS/MS-ISAC is unaware of when the actors may begin targeting, but based on previous incidents, Vikingdom predominantly targets state, local, tribal, and territorial (SLTT) government websites, so it is likely that if they conduct DDoS attacks they will target at least some SLTT government websites. CIS recommends that previous victims of Vikingdom targeting should be especially aware of this threat, as Vikingdom regularly re-targets websites.

(U//LES) Between April and May 2015, Vikingdom claimed, via social media posts, 68 DDoS attacks against SLTT government websites in 34 states. The affected entities reported to MS-ISAC that Vikingdom primarily utilizes Transmission Control Protocol (TCP) Synchronize (SYN) floods, amplification attacks, and high volumes of traffic over port 80/User Datagram Protocol (UDP). The amplification techniques observed include Simple Service Directory Protocol (SSDP) attacks over port 1900/UDP and Network Time Protocol (NTP) attacks over port 123/UDP. Additionally, MS-ISAC has received reports of TCP SYN flood attacks over ports 22 and 25. MS-ISAC members reported attack sizes were generally between 5Gbps and 13Gbps, and that the downtime as the result of the attacks was generally between 15 minutes and 2 hours. The duration of the attacks appears largely dependent upon entity response times and what type of DDoS mitigation was implemented.

TECHNICAL RECOMMENDATIONS: CIS/MS-ISAC strongly recommends the following procedures as a precautionary measure to organizations who feel they may be targeted by DDoS attacks. The CIS "Guide to DDoS Attacks," which includes additional recommendations for identifying and mitigating different types of attacks can be found at:

<https://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks8.pdf>.

Source: Center for Internet Security

Select Federal Products/Reports Recently Released

Product Title / Hyperlink	Product Type	Portal	Release Date	Overall Classification
(U//FOUO) US Southwest Border Drug Update, Fourth Quarter CY 2014	DHS I&A Reference Aid	HSIN	21-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 14-20 May 2015	Weekly Open Source Compilation	HSIN	21-May-15	U//FOUO
(U//FOUO) Syria-Based US and UK Persons' Public Social Media Activity Effective but Provides Terrorism Prevention Opportunities	DHS I&A Intelligence Assessment	HSIN	20-May-15	U//FOUO

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED// LAW ENFORCEMENT SENSITIVE

(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	17-May-15	U//LES
(U) ALLIANCE Magazine: Partnerships in Domestic Counterterrorism	NCTC CT Community Resource	HSIN	15-May-15	U//FOUO
(U//FOUO) Emergency Service Agencies Victimized by Ransomware	Roll Call Release (RCR)	HSIN	15-May-15	U//FOUO
(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot	DHS I&A Intelligence Assessment	HSIN	13-May-15	U//FOUO
(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	8-May-15	U//LES
(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices	Roll Call Release (RCR)	HSIN	8-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 28 April -5 May 2015	Weekly Open Source Compilation	HSIN	6-May-15	U//FOUO

(U//FOUO) HSIN Access: Request membership via email to HSIN at helpdesk@dhs.gov or call 1-866-430-0162. Please include the community of interest (Intelligence and Analysis, Law Enforcement, Emergency Management, Critical Sectors, or Multi-Mission Agencies) to which you require membership, along with full name, official email address, organization, supervisor's name, and a phone number.

(U//FOUO) LEO Access (must belong to a Law Enforcement Agency): Visit LEO.gov click on "LEO Membership Criteria" and then "LEO User Application" or contact the LEO helpdesk at 1-888-334-4536 or via email at helpdesk@leo.gov.

(U//FOUO) If your agency is interested in a product listed above and does not have access to the specific portal the product is located on, please contact the IIFC at 866-400-4432 or iifc@iifc.in.gov.

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



Violent Outlaw Motorcycle Gang (OMG) Encounter in Waco, Texas

(U//FOUO) On 17 May 2015 violence erupted at a restaurant in Waco, TX between rival motorcycle gangs. The incident left nine OMG members dead and 18 wounded. Over 170 OMG members were arrested and charged with engaging in organized crime and could possibly be charged with capital murder.

(U//FOUO) Photos released by the media show members of the Bandidos, Cossacks, and Scimitars OMGs. Law enforcement advised the media there were at least five OMGs involved in the incident, but have not released their names.

(U//FOUO) There are conflicting reports on how the incident started. Initially knives, brass knuckles, and chains were used, but the incident quickly escalated with the use of firearms. Law enforcement was already monitoring the location due to the presence of OMGs and the possibility of violence. When the fight continued in the parking lot, some of the OMGs turned their weapons toward law enforcement. Law enforcement engaged those with weapons and quickly took control. No one other than OMG members were killed or injured.

(U//LES) Analyst Note: INGangNetwork lists the Cossacks and various other OMGs (i.e., Hells Angels, Outlaws, Sons of Silence, etc.) operating in Indiana. The INGangNetwork did not list the Bandidos or Scimitars, but this does not mean these groups might not be traveling through or potentially trying to establish chapters in the state.

(U//LES) Analyst Note: The Cossacks are believed to be aligned with Hells Angels. Hells Angels are rivals of the Bandidos. Texas Joint Crime Information Center (TJCIC) issued a bulletin in March 2015 outlining the growing tension between the Cossacks and Bandidos.

(U//LES) Analyst Note: The IIFC has no information law enforcement in Indiana will be targeted by OMGs due to this incident in Texas. Law enforcement should be aware members of the Cossacks and other OMGs might be traveling through the state for funerals that will be held for the OMG members killed. The IIFC does not have funeral information at this time.

Source: <http://www.cnn.com/2015/05/20/us/texas-biker-gang-shooting-san-antonio-police-martin-lewis/index.html>

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//FOUO) The IIFC encourages security personnel and the public to be aware of the following suspicious behaviors that are believed to be precursors to possible criminal/terroristic activity, including criminal gang activities:

- Surveillance
- Elicitation
- Tests of Security
- Fund Raising
- Acquiring of Supplies
- Suspicious people who appear out of place
- Dry runs
- Deploying assets or positioning of people

(U) Participation in the INGangNetwork

(U) INGangNetwork is offered to any member of the law enforcement and criminal justice community with the need-to-know and a right-to-know gang criminal intelligence.

(U) How to become a member:

(U) Visit the IIFC website at www.in.gov/iifc and click on the INGangNetwork resource link located to the left of the page.

(U) Once the INGangNetwork page loads, click on the [INGangNetwork Application Packet](#) link to download the membership instructions page and the application materials.

IIFC MISSION STATEMENT

The mission of the Indiana Intelligence Fusion Center is to collect, evaluate, analyze and disseminate information and intelligence regarding criminal and terrorist activity in the State of Indiana while following Fair Information Practices to ensure the rights and privacy of citizens.

Executive Director
Jay Nawrocki
jnawrocki@iifc.in.gov
(317) 233-6953

Deputy Director of Intelligence and Analysis
Dan Rose
drose@iifc.IN.gov
(317) 234-4683

Law Enforcement Coordinator
Max Reynolds
maxreynolds@iifc.IN.gov
(317) 234-6653

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.



Customer Satisfaction Survey

Fax to: 317-234-4749

Dear IIFC Customer:

In an effort to ensure quality service and to meet the needs of our customers, we are asking that you please take a few moments to complete this survey. Your feedback will greatly aid our efforts in providing you with the necessary information to accomplish your mission.

Bulletin: 21 May 2015 – PN59976

Please Check the appropriate box.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
This product provided useful information.					
This product provided the level of detail I require.					
This product contained timely information.					
This product provided me with information I do not get from any other source.					
This product affected operations or policy decisions.					
Overall, I am satisfied with this product.					

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

FW: Weekly Bulletin

To: (pbmurray@nilea.com), Al Williamson (awilliamson@isp.in.gov), Alex Kenworthy (akenworthy@marionindiana.us), Andrew Paull (apaull@emichigancity.com), Brett Swanson (bswanson@lcsso.in.gov), Brian Camadeca (bcamadeca@lakecountysheriff.com), cgootee@hammondpolice.com, Chad Crosby (ccrosby@porterco-ps.org), Chanto Iverson (Chanto_Iverson@isp.state.il.us), Christopher Faigh (christopher.faigh@elkhartpolice.org), Corey McKinney (cmckinney@idoc.in.gov), Cynthia Guest (cguest@co.st-joseph.in.us), Dave Hein (dpd22@aol.com), Dave Rybicki (drybicki@stjohnin.com), David Veschak (David_Veschak@csx.com), Dion Campbell (dcampbell@emichigancity.com), Edward A. Rysiewicz (edward.rysiewicz@usdoj.gov), Eric Wiseman (ewiseman@porterco-ps.org), Erik Holloway, Juan Diaz (Sheriff), Gene Hopkins, J. R. Smith (jrsmith@doc.in.gov), Jake Zygmuntowski (jake_zygmuntowski@csx.com), James Donohue, Jamie Co (jcopollo@chestertonin.org), Jeffrey Cook (jcook@schererville.org), Jeremy Chavez (jdcpc67@yahoo.com), jharris@lakecountysheriff.com, John Cordova (jcordova@valpopd.com), John Eagan (jeagan@igc.in.gov), Justine Pond (jpond@marion.k12.in.us), Karl Grimmer (karl_grimmer@csx.com), Karl Hadayag (kmadayag@igc.in.gov), Karl Miller (Karl.miller@elkhartpolice.org), Kenneth Forsythe (kforsythe@lc.hidta.net), Kenneva Mapps (klmapps@idoc.in.gov), Kent Wilson (kwilson@marionindiana.us), Kristopher Adams (krisadamslcpd@yahoo.com), Larry McKinley (slowmotion1378@comcast.net), Laura Lara (llara@igc.in.gov), Lorena Butler (Sheriff), 'lthoma@milwaukee.gov', Marvin Giles (mgiles@idoc.in.gov), Michael Drohosky (mdrohosky@igc.in.gov), Mike Cain (dpdmike@gmail.com), mschmidt@hammondpolice.com, Nathan Battleday (nbattleday@lcsso.in.gov), Nick Yoder (nyoder@co.adams.in.us), Patricia Yelkich (pay1254@sbcglobal.net), Patrick Quinn (patrick.quinn@chicagopolice.org), pcicero@lcsso.in.gov, Raymond K. Humphrey (rhumphrey@isp.in.gov), Richard Spicer (rspicer@valpopd.com), Sgt. Juan Beltran (juan.beltran@leo.gov), Shawn O'Keefe (sokeefe@lakecountysheriff.com), Stephen Bouffard (Sheriff), Steve Scheckel, Tim Felver (tfelver@marionindiana.us), Timothy Shortt (tshortt@lcsso.in.gov), Tom Stinson (vstinson@idoc.in.gov), Tyese Boone (tlboone@idoc.in.gov), Watchcenter (Watchcenter@lc.hidta.net), William Poling (wpoling@igc.in.gov), Brett Scheffel, Brian Ayersman, Brian Bernardino, Brian Hernandez, Bryan Oberc, Dan Broelmann, Daniel Croyle, David Foulkes, David Meyers, Dean Miller, Donald Lindemulder, Gabriel Isenblatter, Jack Deleeuw, James Ghrist, Joseph Newton, Joseph Pacheco, Joseph Wells, Justin Goudreau, Kevin Cooley, Mark Ashcraft, Marshall Van Schouwen, Michael Silsby, Mike Janiga, Nathan Martin, Nolan Archer, Omar Padilla, Ryan Vassar, Spencer Lemmons, Thomas Kuhlenschmidt, Tyler Niven

Sent: May 22, 2015 9:53:46 AM CDT

Received: May 22, 2015 9:54:14 AM CDT

FW: Weekly Bulletin

To: (pbmurray@nilea.com), Al Williamson (awilliamson@isp.in.gov), Alex Kenworthy (akenworthy@marionindiana.us), Andrew Paull (apaul@emichigancity.com), Brett Swanson (bswanson@lcsso.in.gov), Brian Camadeca (bcamadeca@lakecountysheriff.com), cgootee@hammondpolice.com, Chad Crosby (ccrosby@porterco-ps.org), Chanto Iverson (Chanto_Iverson@isp.state.il.us), Christopher Faigh (christopher.faigh@elkhartpolice.org), Corey McKinney (cmckinney@idoc.in.gov), Cynthia Guest (cguest@co.st-joseph.in.us), Dave Hein (dpd22@aol.com), Dave Rybicki (drybicki@stjohnin.com), David Veschak (David_Veschak@csx.com), Dion Campbell (dcampbell@emichigancity.com), Edward A. Rysiewicz (edward.rysiewicz@usdoj.gov), Eric Wiseman (ewiseman@porterco-ps.org), Erik Holloway, Juan Diaz (Sheriff), Gene Hopkins, J. R. Smith (jrsmith@doc.in.gov), Jake Zygmuntowski (jake_zygmuntowski@csx.com), James Donohue, Jamie Co (jcopollo@chestertonin.org), Jeffrey Cook (jcook@schererville.org), Jeremy Chavez (jdcpc67@yahoo.com), jharris@lakecountysheriff.com, John Cordova (jcordova@valpopd.com), John Eagan (jeagan@igc.in.gov), Justine Pond (jpond@marion.k12.in.us), Karl Grimmer (karl_grimmer@csx.com), Karl Hadayag (kmadayag@igc.in.gov), Karl Miller (Karl.miller@elkhartpolice.org), Kenneth Forsythe (kforsythe@lc.hidta.net), Kenneva Mapps (klmapps@idoc.in.gov), Kent Wilson (kwilson@marionindiana.us), Kristopher Adams (krisadamslcpd@yahoo.com), Larry McKinley (slowmotion1378@comcast.net), Laura Lara (llara@igc.in.gov), Lorena Butler (Sheriff), 'lthoma@milwaukee.gov', Marvin Giles (mgiles@idoc.in.gov), Michael Drohosky (mdrohosky@igc.in.gov), Mike Cain (dpdmike@gmail.com), mschmidt@hammondpolice.com, Nathan Battleday (nbattleday@lcsso.in.gov), Nick Yoder (nyoder@co.adams.in.us), Patricia Yelkich (pay1254@sbcglobal.net), Patrick Quinn (patrick.quinn@chicagopolice.org), pcicero@lcsso.in.gov, Raymond K. Humphrey (rhumphrey@isp.in.gov), Richard Spicer (rspicer@valpopd.com), Sgt. Juan Beltran (juan.beltran@leo.gov), Shawn O'Keefe (sokeefe@lakecountysheriff.com), Stephen Bouffard (Sheriff), Steve Scheckel, Tim Felver (tfelver@marionindiana.us), Timothy Shortt (tshortt@lcsso.in.gov), Tom Stinson (vstinson@idoc.in.gov), Tyese Boone (tlboone@idoc.in.gov), Watchcenter (Watchcenter@lc.hidta.net), William Poling (wpoling@igc.in.gov), Brett Scheffel, Brian Ayersman, Brian Bernardino, Brian Hernandez, Bryan Oberc, Dan Broelmann, Daniel Croyle, David Foulkes, David Meyers, Dean Miller, Donald Lindemulder, Gabriel Isenblatter, Jack Deleeuw, James Ghrist, Joseph Newton, Joseph Pacheco, Joseph Wells, Justin Goudreau, Kevin Cooley, Mark Ashcraft, Marshall Van Schouwen, Michael Silsby, Mike Janiga, Nathan Martin, Nolan Archer, Omar Padilla, Ryan Vassar, Spencer Lemmons, Thomas Kuhlenschmidt, Tyler Niven, donotreply@isp.state.il.us

Cc: Cyber_Security@isp.state.il.us

Sent: May 22, 2015 9:53:46 AM CDT

Received: May 22, 2015 9:54:01 AM CDT



INDIANA INTELLIGENCE FUSION CENTER

302 W. Washington St. Room E-243, Indianapolis, IN 46201

Phone: 866-400-4432; Fax: 317-234-4749

Email: iifc@iifc.in.gov

Intelligence Bulletin

21 May 2015

Information Cutoff Date –21 May 2015

INSIDE THIS BULLETIN:

- Officer Awareness: President Obama Signs National Blue Alert Act—P. 2
- RFI: Edinburgh (IN) PD Seeking Agencies with Info. on Recovered Semi-Tractor Filter—P. 2-3
- RFI: Carmel (IN) PD Seeking Theft Suspects—P. 3
- Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Govt Targeting—P. 3-4
- Select Federal Products/Reports Recently Released—P. 4-5
- STATE—INGangNetwork —P. 6-7
- CUSTOMER SATISFACTION SURVEY— P. 8

UPCOMING SIGNIFICANT EVENTS/DATES:

23 May 2015: 500 Festival Parade—Indianapolis, IN

24 May 2015: Indianapolis 500—Speedway, IN

****** If your agency knows of any upcoming events where large crowds are expected and would like them included in the bulletin for awareness purposes, please email information to iifc@iifc.in.gov with the subject line WEEKLY INTELLIGENCE BULLETIN. ******

PN59976

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

Officer Awareness: President Obama Signs National Blue Alert Act

(U) President Barack OBAMA has signed into law a measure to create a nationwide alert system to help catch anyone who injures, kills, or who has made an imminent or credible threat to cause serious injury or death to a law enforcement officer.

(U) The new system would be similar to the Amber Alerts used to find abducted children.

(U) The bill is named for New York City police officers Rafael RAMOS and Wenjian LIU, who were shot and killed in Brooklyn, NY days before Christmas in 2014 by a man who later killed himself. The killer posted threats to law enforcement on social media before the attack. Implementing a nationwide Blue Alert system will help to ensure that information on credible threats, like those posted by the individual who killed detectives RAMOS and LIU, is widely disseminated so that officers have advanced warning, and can apprehend the criminal before he or she can do more harm.

(U) The bill was so uncontroversial that it passed both the House and the Senate by voice vote.

Source: bluealert.us; www.policeone.com

RFI: Edinburgh (IN) Police Department Seeking Agencies with Information on Recovered Semi-Tractor Filter

(U//LES) The Edinburgh (IN) Police Department is seeking agencies that may have information on the semi-tractor filter pictured below that was recovered during a traffic arrest that occurred on 15 May 2015 in Edinburgh, IN. The suspect that was arrested thought the filter was a catalytic converter.



This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//LES) Any agency with thefts possibly connected to the above pictured filter should contact Det. Robert CROCKER; Edinburgh Police Department; 812-526-2636 or rcrocker@edinburgh.in.us.

Source: Edinburgh Police Department

RFI: Carmel (IN) Police Department Seeking Theft Suspects

(U//LES) The Carmel (IN) Police Department is seeking the three suspects pictured below in reference to a theft investigation. The three suspects worked together to commit a short change scam that occurred on 28 April 2015 at a Village Pantry convenience store located in Carmel, IN.

(U//LES) The first suspect entered the store, made a small purchase, and left. The second suspect then entered and proceeded to the register where he began an unknown transaction. The third suspect then distracted an employee at the checkout area. The first suspect returned and made a drink at the fountain machine. He then dropped the drink causing the store manager to walk over and clean up the spill. The second suspect then completed a short change theft at the register by confusing the remaining clerk.



(U//LES) Any agency with similar incidents or similar suspects should contact Det. T. MCINTYRE; Carmel Police Department; 317-571-2728 or tmcintyre@carmel.in.gov.

Source: Carmel Police Department

Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Government Targeting

(U//LES) On 16 May 2015 actors associated with Vikingdom posted a warning on Twitter stating that "U.S. websites are going to be under a massive ddos attack so watch out!" This warning was followed by

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

a post early on 18 May 2015 using the hashtag "#DominateAmerica." CIS/MS-ISAC is unaware of when the actors may begin targeting, but based on previous incidents, Vikingdom predominantly targets state, local, tribal, and territorial (SLTT) government websites, so it is likely that if they conduct DDoS attacks they will target at least some SLTT government websites. CIS recommends that previous victims of Vikingdom targeting should be especially aware of this threat, as Vikingdom regularly re-targets websites.

(U//LES) Between April and May 2015, Vikingdom claimed, via social media posts, 68 DDoS attacks against SLTT government websites in 34 states. The affected entities reported to MS-ISAC that Vikingdom primarily utilizes Transmission Control Protocol (TCP) Synchronize (SYN) floods, amplification attacks, and high volumes of traffic over port 80/User Datagram Protocol (UDP). The amplification techniques observed include Simple Service Directory Protocol (SSDP) attacks over port 1900/UDP and Network Time Protocol (NTP) attacks over port 123/UDP. Additionally, MS-ISAC has received reports of TCP SYN flood attacks over ports 22 and 25. MS-ISAC members reported attack sizes were generally between 5Gbps and 13Gbps, and that the downtime as the result of the attacks was generally between 15 minutes and 2 hours. The duration of the attacks appears largely dependent upon entity response times and what type of DDoS mitigation was implemented.

TECHNICAL RECOMMENDATIONS: CIS/MS-ISAC strongly recommends the following procedures as a precautionary measure to organizations who feel they may be targeted by DDoS attacks. The CIS "Guide to DDoS Attacks," which includes additional recommendations for identifying and mitigating different types of attacks can be found at:

<https://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks8.pdf>.

Source: Center for Internet Security

Select Federal Products/Reports Recently Released

Product Title / Hyperlink	Product Type	Portal	Release Date	Overall Classification
(U//FOUO) US Southwest Border Drug Update, Fourth Quarter CY 2014	DHS I&A Reference Aid	HSIN	21-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 14-20 May 2015	Weekly Open Source Compilation	HSIN	21-May-15	U//FOUO
(U//FOUO) Syria-Based US and UK Persons' Public Social Media Activity Effective but Provides Terrorism Prevention Opportunities	DHS I&A Intelligence Assessment	HSIN	20-May-15	U//FOUO

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED// LAW ENFORCEMENT SENSITIVE

(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	17-May-15	U//LES
(U) ALLIANCE Magazine: Partnerships in Domestic Counterterrorism	NCTC CT Community Resource	HSIN	15-May-15	U//FOUO
(U//FOUO) Emergency Service Agencies Victimized by Ransomware	Roll Call Release (RCR)	HSIN	15-May-15	U//FOUO
(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot	DHS I&A Intelligence Assessment	HSIN	13-May-15	U//FOUO
(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	8-May-15	U//LES
(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices	Roll Call Release (RCR)	HSIN	8-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 28 April -5 May 2015	Weekly Open Source Compilation	HSIN	6-May-15	U//FOUO

(U//FOUO) HSIN Access: Request membership via email to HSIN at helpdesk@dhs.gov or call 1-866-430-0162. Please include the community of interest (Intelligence and Analysis, Law Enforcement, Emergency Management, Critical Sectors, or Multi-Mission Agencies) to which you require membership, along with full name, official email address, organization, supervisor's name, and a phone number.

(U//FOUO) LEO Access (must belong to a Law Enforcement Agency): Visit LEO.gov click on "LEO Membership Criteria" and then "LEO User Application" or contact the LEO helpdesk at 1-888-334-4536 or via email at helpdesk@leo.gov.

(U//FOUO) If your agency is interested in a product listed above and does not have access to the specific portal the product is located on, please contact the IIFC at 866-400-4432 or iifc@iifc.in.gov.

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



Violent Outlaw Motorcycle Gang (OMG) Encounter in Waco, Texas

(U//FOUO) On 17 May 2015 violence erupted at a restaurant in Waco, TX between rival motorcycle gangs. The incident left nine OMG members dead and 18 wounded. Over 170 OMG members were arrested and charged with engaging in organized crime and could possibly be charged with capital murder.

(U//FOUO) Photos released by the media show members of the Bandidos, Cossacks, and Scimitars OMGs. Law enforcement advised the media there were at least five OMGs involved in the incident, but have not released their names.

(U//FOUO) There are conflicting reports on how the incident started. Initially knives, brass knuckles, and chains were used, but the incident quickly escalated with the use of firearms. Law enforcement was already monitoring the location due to the presence of OMGs and the possibility of violence. When the fight continued in the parking lot, some of the OMGs turned their weapons toward law enforcement. Law enforcement engaged those with weapons and quickly took control. No one other than OMG members were killed or injured.

(U//LES) Analyst Note: INGangNetwork lists the Cossacks and various other OMGs (i.e., Hells Angels, Outlaws, Sons of Silence, etc.) operating in Indiana. The INGangNetwork did not list the Bandidos or Scimitars, but this does not mean these groups might not be traveling through or potentially trying to establish chapters in the state.

(U//LES) Analyst Note: The Cossacks are believed to be aligned with Hells Angels. Hells Angels are rivals of the Bandidos. Texas Joint Crime Information Center (TJCIC) issued a bulletin in March 2015 outlining the growing tension between the Cossacks and Bandidos.

(U//LES) Analyst Note: The IIFC has no information law enforcement in Indiana will be targeted by OMGs due to this incident in Texas. Law enforcement should be aware members of the Cossacks and other OMGs might be traveling through the state for funerals that will be held for the OMG members killed. The IIFC does not have funeral information at this time.

Source: <http://www.cnn.com/2015/05/20/us/texas-biker-gang-shooting-san-antonio-police-martin-lewis/index.html>

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//FOUO) The IIFC encourages security personnel and the public to be aware of the following suspicious behaviors that are believed to be precursors to possible criminal/terroristic activity, including criminal gang activities:

- Surveillance
- Elicitation
- Tests of Security
- Fund Raising
- Acquiring of Supplies
- Suspicious people who appear out of place
- Dry runs
- Deploying assets or positioning of people

(U) Participation in the INGangNetwork

(U) INGangNetwork is offered to any member of the law enforcement and criminal justice community with the need-to-know and a right-to-know gang criminal intelligence.

(U) How to become a member:

(U) Visit the IIFC website at www.in.gov/iifc and click on the INGangNetwork resource link located to the left of the page.

(U) Once the INGangNetwork page loads, click on the [INGangNetwork Application Packet](#) link to download the membership instructions page and the application materials.

IIFC MISSION STATEMENT

The mission of the Indiana Intelligence Fusion Center is to collect, evaluate, analyze and disseminate information and intelligence regarding criminal and terrorist activity in the State of Indiana while following Fair Information Practices to ensure the rights and privacy of citizens.

Executive Director
Jay Nawrocki
jnawrocki@iifc.in.gov
(317) 233-6953

Deputy Director of Intelligence and Analysis
Dan Rose
drose@iifc.IN.gov
(317) 234-4683

Law Enforcement Coordinator
Max Reynolds
maxreynolds@iifc.IN.gov
(317) 234-6653

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.



Customer Satisfaction Survey

Fax to: 317-234-4749

Dear IIFC Customer:

In an effort to ensure quality service and to meet the needs of our customers, we are asking that you please take a few moments to complete this survey. Your feedback will greatly aid our efforts in providing you with the necessary information to accomplish your mission.

Bulletin: 21 May 2015 – PN59976

Please Check the appropriate box.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
This product provided useful information.					
This product provided the level of detail I require.					
This product contained timely information.					
This product provided me with information I do not get from any other source.					
This product affected operations or policy decisions.					
Overall, I am satisfied with this product.					

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

FW: Weekly Bulletin

To: Brian Duffy (Sheriff)
Sent: May 22, 2015 10:11:52 AM CDT
Received: May 22, 2015 10:11:53 AM CDT



INDIANA INTELLIGENCE FUSION CENTER

302 W. Washington St. Room E-243, Indianapolis, IN 46201

Phone: 866-400-4432; Fax: 317-234-4749

Email: iifc@iifc.in.gov

Intelligence Bulletin

21 May 2015

Information Cutoff Date –21 May 2015

INSIDE THIS BULLETIN:

- Officer Awareness: President Obama Signs National Blue Alert Act—P. 2
- RFI: Edinburgh (IN) PD Seeking Agencies with Info. on Recovered Semi-Tractor Filter—P. 2-3
- RFI: Carmel (IN) PD Seeking Theft Suspects—P. 3
- Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Govt Targeting—P. 3-4
- Select Federal Products/Reports Recently Released—P. 4-5
- STATE—INGangNetwork —P. 6-7
- CUSTOMER SATISFACTION SURVEY— P. 8

UPCOMING SIGNIFICANT EVENTS/DATES:

23 May 2015: 500 Festival Parade—Indianapolis, IN

24 May 2015: Indianapolis 500—Speedway, IN

****** If your agency knows of any upcoming events where large crowds are expected and would like them included in the bulletin for awareness purposes, please email information to iifc@iifc.in.gov with the subject line WEEKLY INTELLIGENCE BULLETIN. ******

PN59976

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

Officer Awareness: President Obama Signs National Blue Alert Act

(U) President Barack OBAMA has signed into law a measure to create a nationwide alert system to help catch anyone who injures, kills, or who has made an imminent or credible threat to cause serious injury or death to a law enforcement officer.

(U) The new system would be similar to the Amber Alerts used to find abducted children.

(U) The bill is named for New York City police officers Rafael RAMOS and Wenjian LIU, who were shot and killed in Brooklyn, NY days before Christmas in 2014 by a man who later killed himself. The killer posted threats to law enforcement on social media before the attack. Implementing a nationwide Blue Alert system will help to ensure that information on credible threats, like those posted by the individual who killed detectives RAMOS and LIU, is widely disseminated so that officers have advanced warning, and can apprehend the criminal before he or she can do more harm.

(U) The bill was so uncontroversial that it passed both the House and the Senate by voice vote.

Source: bluealert.us; www.policeone.com

RFI: Edinburgh (IN) Police Department Seeking Agencies with Information on Recovered Semi-Tractor Filter

(U//LES) The Edinburgh (IN) Police Department is seeking agencies that may have information on the semi-tractor filter pictured below that was recovered during a traffic arrest that occurred on 15 May 2015 in Edinburgh, IN. The suspect that was arrested thought the filter was a catalytic converter.



This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//LES) Any agency with thefts possibly connected to the above pictured filter should contact Det. Robert CROCKER; Edinburgh Police Department; 812-526-2636 or rcrocker@edinburgh.in.us.

Source: Edinburgh Police Department

RFI: Carmel (IN) Police Department Seeking Theft Suspects

(U//LES) The Carmel (IN) Police Department is seeking the three suspects pictured below in reference to a theft investigation. The three suspects worked together to commit a short change scam that occurred on 28 April 2015 at a Village Pantry convenience store located in Carmel, IN.

(U//LES) The first suspect entered the store, made a small purchase, and left. The second suspect then entered and proceeded to the register where he began an unknown transaction. The third suspect then distracted an employee at the checkout area. The first suspect returned and made a drink at the fountain machine. He then dropped the drink causing the store manager to walk over and clean up the spill. The second suspect then completed a short change theft at the register by confusing the remaining clerk.



(U//LES) Any agency with similar incidents or similar suspects should contact Det. T. MCINTYRE; Carmel Police Department; 317-571-2728 or tmcintyre@carmel.in.gov.

Source: Carmel Police Department

Cyber Awareness: Vikingdom Issues New Threat Likely Leading to SLTT Government Targeting

(U//LES) On 16 May 2015 actors associated with Vikingdom posted a warning on Twitter stating that "U.S. websites are going to be under a massive ddos attack so watch out!" This warning was followed by

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

a post early on 18 May 2015 using the hashtag "#DominateAmerica." CIS/MS-ISAC is unaware of when the actors may begin targeting, but based on previous incidents, Vikingdom predominantly targets state, local, tribal, and territorial (SLTT) government websites, so it is likely that if they conduct DDoS attacks they will target at least some SLTT government websites. CIS recommends that previous victims of Vikingdom targeting should be especially aware of this threat, as Vikingdom regularly re-targets websites.

(U//LES) Between April and May 2015, Vikingdom claimed, via social media posts, 68 DDoS attacks against SLTT government websites in 34 states. The affected entities reported to MS-ISAC that Vikingdom primarily utilizes Transmission Control Protocol (TCP) Synchronize (SYN) floods, amplification attacks, and high volumes of traffic over port 80/User Datagram Protocol (UDP). The amplification techniques observed include Simple Service Directory Protocol (SSDP) attacks over port 1900/UDP and Network Time Protocol (NTP) attacks over port 123/UDP. Additionally, MS-ISAC has received reports of TCP SYN flood attacks over ports 22 and 25. MS-ISAC members reported attack sizes were generally between 5Gbps and 13Gbps, and that the downtime as the result of the attacks was generally between 15 minutes and 2 hours. The duration of the attacks appears largely dependent upon entity response times and what type of DDoS mitigation was implemented.

TECHNICAL RECOMMENDATIONS: CIS/MS-ISAC strongly recommends the following procedures as a precautionary measure to organizations who feel they may be targeted by DDoS attacks. The CIS "Guide to DDoS Attacks," which includes additional recommendations for identifying and mitigating different types of attacks can be found at:

<https://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks8.pdf>.

Source: Center for Internet Security

Select Federal Products/Reports Recently Released

Product Title / Hyperlink	Product Type	Portal	Release Date	Overall Classification
(U//FOUO) US Southwest Border Drug Update, Fourth Quarter CY 2014	DHS I&A Reference Aid	HSIN	21-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 14-20 May 2015	Weekly Open Source Compilation	HSIN	21-May-15	U//FOUO
(U//FOUO) Syria-Based US and UK Persons' Public Social Media Activity Effective but Provides Terrorism Prevention Opportunities	DHS I&A Intelligence Assessment	HSIN	20-May-15	U//FOUO

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED// LAW ENFORCEMENT SENSITIVE

(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	17-May-15	U//LES
(U) ALLIANCE Magazine: Partnerships in Domestic Counterterrorism	NCTC CT Community Resource	HSIN	15-May-15	U//FOUO
(U//FOUO) Emergency Service Agencies Victimized by Ransomware	Roll Call Release (RCR)	HSIN	15-May-15	U//FOUO
(U//FOUO) Future ISIL Operations in the West Could Resemble Disrupted Belgian Plot	DHS I&A Intelligence Assessment	HSIN	13-May-15	U//FOUO
(U//FOUO) C-Note Bulk Cash Smuggling Weekly Report	ICE HSI Bulk Cash Smuggling Center (BCSC) Weekly	HSIN	8-May-15	U//LES
(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices	Roll Call Release (RCR)	HSIN	8-May-15	U//FOUO
(U) NCTC Counterterrorism Weekly, 28 April -5 May 2015	Weekly Open Source Compilation	HSIN	6-May-15	U//FOUO

(U//FOUO) HSIN Access: Request membership via email to HSIN at helpdesk@dhs.gov or call 1-866-430-0162. Please include the community of interest (Intelligence and Analysis, Law Enforcement, Emergency Management, Critical Sectors, or Multi-Mission Agencies) to which you require membership, along with full name, official email address, organization, supervisor's name, and a phone number.

(U//FOUO) LEO Access (must belong to a Law Enforcement Agency): Visit LEO.gov click on "LEO Membership Criteria" and then "LEO User Application" or contact the LEO helpdesk at 1-888-334-4536 or via email at helpdesk@leo.gov.

(U//FOUO) If your agency is interested in a product listed above and does not have access to the specific portal the product is located on, please contact the IIFC at 866-400-4432 or iifc@iifc.in.gov.

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



Violent Outlaw Motorcycle Gang (OMG) Encounter in Waco, Texas

(U//FOUO) On 17 May 2015 violence erupted at a restaurant in Waco, TX between rival motorcycle gangs. The incident left nine OMG members dead and 18 wounded. Over 170 OMG members were arrested and charged with engaging in organized crime and could possibly be charged with capital murder.

(U//FOUO) Photos released by the media show members of the Bandidos, Cossacks, and Scimitars OMGs. Law enforcement advised the media there were at least five OMGs involved in the incident, but have not released their names.

(U//FOUO) There are conflicting reports on how the incident started. Initially knives, brass knuckles, and chains were used, but the incident quickly escalated with the use of firearms. Law enforcement was already monitoring the location due to the presence of OMGs and the possibility of violence. When the fight continued in the parking lot, some of the OMGs turned their weapons toward law enforcement. Law enforcement engaged those with weapons and quickly took control. No one other than OMG members were killed or injured.

(U//LES) Analyst Note: INGangNetwork lists the Cossacks and various other OMGs (i.e., Hells Angels, Outlaws, Sons of Silence, etc.) operating in Indiana. The INGangNetwork did not list the Bandidos or Scimitars, but this does not mean these groups might not be traveling through or potentially trying to establish chapters in the state.

(U//LES) Analyst Note: The Cossacks are believed to be aligned with Hells Angels. Hells Angels are rivals of the Bandidos. Texas Joint Crime Information Center (TJCIC) issued a bulletin in March 2015 outlining the growing tension between the Cossacks and Bandidos.

(U//LES) Analyst Note: The IIFC has no information law enforcement in Indiana will be targeted by OMGs due to this incident in Texas. Law enforcement should be aware members of the Cossacks and other OMGs might be traveling through the state for funerals that will be held for the OMG members killed. The IIFC does not have funeral information at this time.

Source: <http://www.cnn.com/2015/05/20/us/texas-biker-gang-shooting-san-antonio-police-martin-lewis/index.html>

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES.** Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

(U//FOUO) The IIFC encourages security personnel and the public to be aware of the following suspicious behaviors that are believed to be precursors to possible criminal/terroristic activity, including criminal gang activities:

- Surveillance
- Elicitation
- Tests of Security
- Fund Raising
- Acquiring of Supplies
- Suspicious people who appear out of place
- Dry runs
- Deploying assets or positioning of people

(U) Participation in the INGangNetwork

(U) INGangNetwork is offered to any member of the law enforcement and criminal justice community with the need-to-know and a right-to-know gang criminal intelligence.

(U) How to become a member:

(U) Visit the IIFC website at www.in.gov/iifc and click on the INGangNetwork resource link located to the left of the page.

(U) Once the INGangNetwork page loads, click on the [INGangNetwork Application Packet](#) link to download the membership instructions page and the application materials.

IIFC MISSION STATEMENT

The mission of the Indiana Intelligence Fusion Center is to collect, evaluate, analyze and disseminate information and intelligence regarding criminal and terrorist activity in the State of Indiana while following Fair Information Practices to ensure the rights and privacy of citizens.

Executive Director
Jay Nawrocki
jnawrocki@iifc.in.gov
(317) 233-6953

Deputy Director of Intelligence and Analysis
Dan Rose
drose@iifc.IN.gov
(317) 234-4683

Law Enforcement Coordinator
Max Reynolds
maxreynolds@iifc.IN.gov
(317) 234-6653

This information is **UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. **NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES**. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.



Customer Satisfaction Survey

Fax to: 317-234-4749

Dear IIFC Customer:

In an effort to ensure quality service and to meet the needs of our customers, we are asking that you please take a few moments to complete this survey. Your feedback will greatly aid our efforts in providing you with the necessary information to accomplish your mission.

Bulletin: 21 May 2015 – PN59976

Please Check the appropriate box.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
This product provided useful information.					
This product provided the level of detail I require.					
This product contained timely information.					
This product provided me with information I do not get from any other source.					
This product affected operations or policy decisions.					
Overall, I am satisfied with this product.					

This information is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies only, unless prior approval from the Indiana Intelligence Fusion Center is obtained. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Indiana Intelligence Fusion Center if you have any questions or need additional information.

Illinois Freedom of Information Act. Request: Criminal Hackers Target Police to Protest Perceived Injustices (Cook County Sheriff)

From: 75700-84621158@requests.muckrock.com
To: ccsso.foiaofficer@cookcountyiil.gov, CCSO FOIAOfficer (Sheriff)
</o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=18fb7119706c4e188b73eff50943de3
9-CCSO FOIAOf>
Sender: 75700-84621158@requests.muckrock.com
Sent: June 21, 2019 12:12:42 PM CDT
Received: June 21, 2019 12:12:57 PM CDT
Attachments: DHS-FBI-HackersTargetPolice.pdf

Cook County Sheriff
FOIA Office
Richard J. Daley Center
50 West Washington Street
Chicago, IL 60602

June 21, 2019

To Whom It May Concern:

Pursuant to the Illinois Freedom of Information Act., I hereby request the following records:

Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 75700-84621158@requests.muckrock.com

Upload documents directly:

https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAaaJnszUVssmdgx6fh2R-tE3U%3A1heN5d%3A6QVm4fNbQBxPfjnUPTdAQqauqWc&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fcook-county-sheriff-719%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-cook-county-sheriff-75700%252F%253Femail%253Dccso.foiaofficer%252540cookcountyil.gov

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 75700

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



ROLL CALL RELEASE

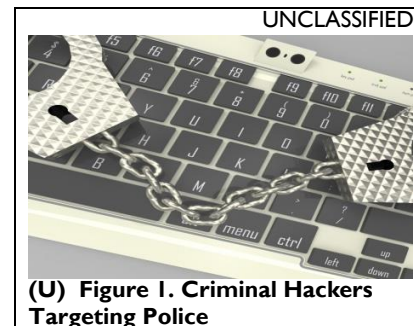
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

Illinois Freedom of Information Act. Request: Criminal Hackers Target Police to Protest Perceived Injustices (Cook County Sheriff)

To: CCSO FOIA Officer (Sheriff)
Sent: June 21, 2019 12:12:42 PM CDT
Received: June 21, 2019 12:12:58 PM CDT

[GovQA] New Request Assignment - R001649-062619

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Eryn.Hedderman@cookcountyil.gov <Eryn.Hedderman@cookcountyil.gov>, Eryn Hedderman (Sheriff) </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=da84f6c14e4a40ffb4b4b24d87e04cef-Eryn T. Hed>
Sent: June 26, 2019 5:07:02 PM CDT
Received: June 26, 2019 5:07:06 PM CDT

A request has been assigned to you: FOIA Request / R001649-062619

Request Information

Assigned Staff: Eryn Hedderman

Status: Received

Create Date: 6/21/2019 8:00:00 AM

Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best

Login to the system and view your request by clicking [HERE](#).

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY

[GovQA] New Request Assignment - R001649-062619

To: Eryn Hedderman (Sheriff)
Sent: June 26, 2019 5:07:02 PM CDT
Received: June 26, 2019 5:07:06 PM CDT

[GovQA] New Request Assignment - R001649-062619

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Elizabeth.Scannell@cookcountyil.gov <Elizabeth.Scannell@cookcountyil.gov>, Elizabeth Scannell (Sheriff) </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e3f5adf1bbdc48c9bd4a9be8268ea25e-Elizabeth S>
Sent: June 26, 2019 5:07:04 PM CDT
Received: June 26, 2019 5:07:07 PM CDT

A request has been assigned to you: FOIA Request / R001649-062619

Request Information

Assigned Staff: Elizabeth Scannell

Status: Received

Create Date: 6/21/2019 8:00:00 AM

Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best

Login to the system and view your request by clicking [HERE](#).

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY

[GovQA] New Request Assignment - R001649-062619

To: Elizabeth Scannell (Sheriff)
Sent: June 26, 2019 5:07:04 PM CDT
Received: June 26, 2019 5:07:08 PM CDT

[GovQA] 1 Day Reminder - R001649-062619

From: Cook County Sheriff's Office <cookcountysheriff@govqa.us>
To: Elizabeth.Scannell@cookcountyil.gov <Elizabeth.Scannell@cookcountyil.gov>, Elizabeth Scannell (Sheriff) </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e3f5adf1bbdc48c9bd4a9be8268ea25e-Elizabeth S>
Sent: June 27, 2019 8:03:50 AM CDT
Received: June 27, 2019 8:03:53 AM CDT

Reminder the following request is due in ONE (1) business days: FOIA Request / R001649-062619
Please log in to the FOIA Request Center to review this request and update as needed.

Request Information

Assigned Staff: Elizabeth Scannell

Status: Received

Create Date: 6/21/2019 8:00:00 AM

Record(s) Requested: To Whom It May Concern: Pursuant to the Illinois Freedom of Information Act., I hereby request the following records: Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it. I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived. The requested documents will be made available to the general public, and this request is not being made for commercial purposes. In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not. Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires. Sincerely, Emma Best

Login to the system and view this request by clicking [View the Request](#)

This is an auto-generated email and has originated from an unmonitored email account. Please DO NOT REPLY

[GovQA] 1 Day Reminder - R001649-062619

To: Elizabeth Scannell (Sheriff)
Sent: June 27, 2019 8:03:50 AM CDT
Received: June 27, 2019 8:03:54 AM CDT